



Command Line Interface Reference

The Cisco SN 5428-2 Storage Router provides three interfaces for operation, configuration, administration, maintenance, and support tasks: command line interface (CLI), web-based GUI, and SNMP.

This chapter documents the storage router CLI. For help on the web-based GUI, point your browser to the storage router's management interface IP address. After logging on, click the Help link to access the online help system.

This chapter provides information about the following CLI topics:

- [About CLI Commands, page 12-1](#)
- [CLI Usage Tips, page 12-1](#)
- [CLI Commands, page 12-2](#)

About CLI Commands

This chapter lists all possible CLI commands. However, the set of CLI commands and keywords that are available to you depends on the level of authority associated with your CLI management session and the deployment option selected for the SN 5428-2 Storage Router during initial configuration.

Use the **show cli** command to view all CLI commands and keywords that are valid for your current CLI management session.

CLI Usage Tips

- Commands and keywords can be truncated at any point after they are unique.
- Use the Tab key to complete the current word.
- Use the question mark (?) key to list all of the options available at that point in the command line.
- CLI commands and keywords are not case-sensitive. Commands and keywords can be entered in any case (including mixed case).
- User-defined strings are case-sensitive. User-defined strings must be entered in the appropriate case (including mixed case). Case for user-defined strings is preserved in the configuration.
- An asterisk (*) at the beginning of the CLI command prompt indicates that the system configuration has been changed but not saved.

CLI Commands

This section lists all CLI commands in alphabetical order. The **no** form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, history, usage guidelines, examples, and related commands.

aaa authentication enable

To configure authentication, authorization and accounting (AAA) authentication services for Administrator mode access to the CLI (via the CLI **enable** command), use the **aaa authentication enable** command. To disable this authentication, use the **no** form of this command.

aaa authentication enable default *services1* [*services2...*]

no aaa authentication enable default

Syntax Description

default	The name of the authentication list. The list name must be <i>default</i> .
<i>services1</i> [<i>services2...</i>]	At least one of the services described in Table 12-1 .

Defaults

If the default list is not configured, only the Administrator mode password is checked. This has the same effect as the following command:

aaa authentication enable default enable

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Administrator mode access (“Enable”) authentication uses AAA authentication services to provide authentication of users that request Administrator mode access to the storage router via the CLI **enable** command. Because the **enable** command does not require you to enter a user name, the special user name *\$enab15\$* is used if RADIUS or TACACS+ servers are used for authentication.

AAA attempts to use each service in the order listed in the default authentication list, until authentication succeeds or fails. If the service fails to find a user name and password match, authentication fails and access is denied. If AAA returns an error (because the RADIUS or TACACS+ server is not available, for example), AAA attempts to use the next service in the list for authentication. To specify that the authentication should succeed even if all methods return an error (not if they return an authentication failure), specify **none** as the final method in the command line. Use the **show aaa** command to display the current authentication lists.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa authentication enable** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.



Note

Enable authentication extends to users accessing the storage router via an FTP session. An FTP session requires the user name *admin* and the password that would be entered for the CLI **enable** command.

In Table 12-1, the **group radius** and **group tacacs+** methods refer to all previously defined RADIUS or TACACS+ servers; the **group name** method refers to a previously defined group of one or more RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the servers, and the **aaa group server radius** and **aaa group server tacacs+** commands to create server groups.

Table 12-1 *aaa authentication enable default services*

Keyword	Description
enable	Uses the configured Administrator mode password for authentication.
group name	Uses a named group of defined RADIUS or TACACS+ servers for authentication, using the user name <i>\$enab15\$</i> .
group radius	Uses the list of all RADIUS servers for authentication, using the user name <i>\$enab15\$</i> .
group tacacs+	Uses the list of all TACACS+ servers for authentication, using the user name <i>\$enab15\$</i> .
monitor	Uses the configured Monitor mode password for authentication.
none	Uses no authentication.

Examples

The following example creates a default AAA authentication list to be used to perform Enable authentication. When Administrator access of the storage router is requested via the CLI **enable** command, AAA first attempts to contact a RADIUS server, using the *\$enab15\$* username and the entered password. If no server is found, AAA returns an error and authentication is performed by checking the entered password against the configured Administrator mode password. If there is no match, authentication fails and you are denied Administrator access.

```
[SN5428-2A] # aaa authentication enable default group radius enable
```

Related Commands

Command	Description
aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
aaa test authentication	Enable testing of the specified AAA authentication list.
debug aaa	Enable debugging for the AAA authentication services.
radius-server host	Configure remote RADIUS servers for AAA authentication services.
restore aaa	Restore AAA authentication services from the named configuration file.
save aaa	Save the current AAA configuration information.
show aaa	Display AAA configuration information.
tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

aaa authentication iscsi

To configure authentication, authorization and accounting (AAA) authentication services for iSCSI authentication of IP hosts requesting access to storage via SCSI routing instances, use the **aaa authentication iscsi** command. To disable this authentication, use the **no** form of this command.

```
aaa authentication iscsi {listname | default} services1 [services2...]
```

```
no aaa authentication iscsi {listname | default}
```

Syntax Description

<i>listname</i>	The name of the authentication list. Enter a maximum of 31 characters.
default	The name of the default authentication list.
<i>services1 [services2...]</i>	At least one of the services described in Table 12-2 .

Defaults

If iSCSI authentication is enabled and the named authentication list is not configured, authentication fails.

If iSCSI authentication is enabled using the default list but the default list is not configured, only the local user database is selected. This has the same effect as the following command:

```
aaa authentication iscsi default local
```

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

iSCSI authentication uses AAA authentication services to provide authentication of IP hosts that request access to storage from SCSI routing instances that have authentication enabled.

AAA attempts to use each service in the order listed in the specified iSCSI authentication list, until authentication succeeds or fails. If the service fails to find a user name match, authentication fails. If AAA returns an error (because the RADIUS or TACACS+ server is not available, for example), AAA attempts to use the next service in the list for authentication.

If either local or local-case is the first service on the iSCSI authentication list and AAA fails to find a user name match, AAA attempts to use the next method on the list for authentication. If the local or local-case service is in any other position on the list and AAA fails to find a user name match, authentication fails and access is denied. If a RADIUS or TACACS+ server fails to find a user name match (regardless of position on the iSCSI authentication list), authentication fails and access is denied.

Use the **show aaa** command to display the current authentication lists.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa authentication iscsi** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

In Table 12-2, the **group radius** and **group tacacs+** methods refer to all previously defined RADIUS or TACACS+ servers; the **group name** method refers to a group of one or more RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the servers, and the **aaa group server radius** and **aaa group server tacacs+** commands to create server groups.

**Note**

A named server group must be defined to be used as an authentication method. However, verification of server groups occurs only at runtime. If a server group is not defined, the authentication process generates error messages and the server group is skipped. This could cause unexpected authentication failures.

Table 12-2 *aaa authentication iscsi services*

Keyword	Description
group name	Uses a named group of defined RADIUS or TACACS+ servers for authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.

If the local authentication service is selected, the user name validation is not case-sensitive. If local-case authentication service is selected, the user name validation is case-sensitive. The password validation for both the local service and the local-case service is case-sensitive.

Examples

The following example creates a new AAA authentication list named *webtest* and enables iSCSI authentication for the SCSI routing instance named *myCompanyWebserver2*, using the *webtest* authentication list. When iSCSI authentication is required, AAA first tries to use the local username database for authentication. If no match is found, AAA attempts to contact a TACACS+ server. If no server is found, AAA returns an error and the IP host is allowed access with no authentication.

```
[SN5428-2A] # aaa authentication iscsi webtest local group tacacs+ none
[SN5428-2A] # scsirouter myCompanyWebserver2 authentication webtest
```


Related Commands	Command	Description
	aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
	aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	debug aaa	Enable debugging for the AAA authentication services.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

aaa authentication login

To configure authentication, authorization and accounting (AAA) authentication services for Monitor mode access to the storage router via the CLI, use the **aaa authentication login** command. To disable this authentication, use the **no** form of this command.

aaa authentication login default *services1* [*services2...*]

no aaa authentication login default

Syntax Description

default	The name of the authentication list. The list name must be <i>default</i> .
<i>services1</i> [<i>services2...</i>]	At least one of the services described in Table 12-3 .

Defaults

If the default list is not configured, only the Monitor mode password is checked. This has the same effect as the following command:

aaa authentication login default monitor



Note

If the default list is not configured, you are only prompted to enter a password; you are not prompted to enter a user name.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Monitor mode access (“Login”) authentication uses AAA authentication services to provide authentication of users that request Monitor mode access to the SN 5428-2 Storage Router via the CLI. A user attempting Monitor mode access of the storage router via the CLI will be prompted for a user name and password.

AAA attempts to use each service in the order listed in the default authentication list, until authentication succeeds or fails. If the service fails to find a user name match, authentication fails. If AAA returns an error (because the RADIUS or TACACS+ server is not available, for example), AAA attempts to use the next service in the list for authentication. To specify that the authentication should succeed even if all methods return an error (not if they return an authentication failure), specify **none** as the final method in the command line.

If either local or local-case is the first service on the default authentication list and AAA fails to find a user name match, AAA attempts to use the next method on the list for authentication. If the local or local-case service is in any other position on the list and AAA fails to find a user name match, authentication fails and access is denied. If a RADIUS or TACACS+ server fails to find a user name match (regardless of position on the default authentication list), authentication fails and access is denied.

If the Enable service is used, the user name is ignored and the password is authenticated against the configured Administrator mode password. If the Monitor service is used, the user name is ignored and the password is authenticated against the configured Monitor mode password.

**Note**

AAA does not provide authentication for access via the GUI (using HTTP or HTTPS).

Use the **show aaa** command to display the current authentication lists.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa authentication login** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

In [Table 12-3](#), the **group radius** and **group tacacs+** methods refer to all previously defined RADIUS or TACACS+ servers; the **group name** method refers to a previously defined group of one or more RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the servers, and the **aaa group server radius** and **aaa group server tacacs+** commands to create server groups.

Table 12-3 *aaa authentication login default services*

Keyword	Description
enable	Uses the configured Administrator mode password for authentication. The user name is ignored.
group name	Uses a named group of defined RADIUS or TACACS+ servers for authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
monitor	Uses the configured Monitor mode password for authentication. The user name is ignored.
none	Uses no authentication.

If the local authentication service is selected, the user name validation is not case-sensitive. If local-case authentication service is selected, the user name validation is case-sensitive. The password validation for both the local service and the local-case service is case-sensitive.

Examples

The following example creates a default AAA authentication list to be used to perform Login authentication. AAA first attempts to contact a RADIUS server. If no server is found, AAA returns an error and authentication is performed by checking the local username database. If no match is found, AAA performs authentication by checking the entered password against the configured Monitor mode password.

```
[SN5428-2A] # aaa authentication login default group radius local monitor
```


Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
	aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
	aaa group server tacacs+	Create a named group of RADIUS servers for AAA authentication services.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	debug aaa	Enable debugging for the AAA authentication services.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

aaa generate password

To generate a long random password, use the **aaa generate password** command.

aaa generate password

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to generate a long random password. From a CLI management session, you can cut and paste this password into other commands or applications, using the conventions appropriate to your specific Telnet or SSH client, or operating system.
-------------------------	--

Examples	The following example generates a long random password:
-----------------	---

```
[SN5428-2A]# aaa generate password  
Password: 28b79da19608342a99642ce92fbdd3114
```

Related Commands	Command	Description
	aaa test authentication	Enable testing of the specified AAA authentication list.
	admin password	Set the login password for administrative access to the storage router management interface.
	monitor password	Set the login password for view-only access to the storage router management interface.
	username password	Add a user name and optional password to the local username database.

aaa group server radius

To create a named group of RADIUS servers to be used for AAA authentication, use the **aaa group server radius** command. To disable an existing group of RADIUS servers, use the **no** form of this command.

```
aaa group server radius name

no aaa group server radius name
```

Syntax Description	<div> <div>name</div> <div>The name of the group of RADIUS servers to be used for AAA authentication. Enter a maximum of 31 characters.</div> </div>	
Defaults	None. All configured RADIUS servers belong to the group named <i>radius</i> .	
Command Modes	Administrator.	
Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Use this command to create a subset of RADIUS servers to be used for AAA authentication. The named group can then be added to a AAA authentication methods list, allowing the specified set of RADIUS servers to be used for authentication. After creating the named group, use the **aaa group server radius server** command to add a RADIUS server to the group.

Use the **radius-server host** command to configure a RADIUS server to be used by the storage router for AAA authentication.

Group names must be unique across the storage router; you cannot have a group of RADIUS servers named *labauth* and a group of TACACS+ servers named *labauth*. The default group name of *radius* includes all configured RADIUS servers.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa group server radius** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Examples

The following example creates a RADIUS server group named *region2*:

```
[SN5428-2A]# aaa group server radius region2
```


Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
	aaa group server radius deadtime	Specify the length of time the storage router can skip a RADIUS server in the named group that is marked as unavailable.
	aaa group server radius server	Add the specified RADIUS server to the named RADIUS server group.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	radius-server deadtime	Specify the length of time the storage router can skip a RADIUS server that is marked as unavailable.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	radius-server key	Sets the global authentication and encryption key for all RADIUS communications between the storage router and the RADIUS daemon.
	radius-server retransmit	Specifies how many times the storage router resends the RADIUS request to a server before giving up.
	radius-server timeout	Sets the interval the storage router waits for a RADIUS server to reply before retransmitting.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.

aaa group server radius deadline

To improve RADIUS response time when some servers might be unavailable, use the **aaa group server radius deadline** command to cause the storage router to skip the unavailable servers in the specified group immediately. To set the dead time to 0, effectively preventing the storage router from skipping any RADIUS server in the specified group, use the **no** form of this command.

aaa group server radius *name* **deadline** *minutes*

no aaa group server radius *name* **deadline**

Syntax Description	<i>name</i>	The name of the group of RADIUS servers. Enter a maximum of 31 characters.
	<i>minutes</i>	The length of time, in minutes, for which a RADIUS server in the specified group is skipped over by the storage router when requesting AAA authentication services, up to a maximum of 1440 minutes (24 hours).

Defaults The dead time is set to zero (0) by default.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Use this command to cause the storage router to mark as “dead” any RADIUS servers in the specified group that fail to respond to authentication requests, thus avoiding the wait for the authentication request to time out before trying the next configured server. A RADIUS server marked as dead is skipped by additional requests for the specified number of minutes, unless all RADIUS servers in the specified list are marked as dead. If all RADIUS servers in a group are marked as dead, the deadline setting is ignored.

This command overrides the global setting that applies to all configured RADIUS servers. If the deadline is not set for a RADIUS server group, the global dead time setting applies.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa group server radius deadline** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Examples

The following example specifies a dead time of five minutes for all RADIUS servers in the group named *region2* that fail to respond to AAA authentication requests:

```
[SN5428-2A]# aaa group server radius region6 deadline 5
```


The following example effectively sets a dead time of zero minutes for all RADIUS servers in the group named *region6*. The global dead time value, if set, will apply to all RADIUS server in the group.

```
[SN5428-2A] # no aaa group server radius region6 deadline
```

Related Commands	Command	Description
	radius-server deadline	Specify the length of time the storage router can skip a RADIUS server that is marked as unavailable.
	show aaa	Display AAA configuration information.

aaa group server radius server

To add a RADIUS server to a named group of RADIUS servers to be used for AAA authentication, use the **aaa group server radius server** command. To remove a RADIUS server from an existing group of RADIUS servers, use the **no** form of this command.

aaa group server radius *name* **server** *ip-address* [**auth-port** *port-number*]

no aaa group server radius *name* **server** *ip-address* [**auth-port** *port-number*]

Syntax Description	<i>name</i>	The name of the group of RADIUS servers. Enter a maximum of 31 characters.
	<i>ip-address</i>	The IP address of the RADIUS server.
	auth-port <i>port-number</i>	(Optional) The UDP destination port for authentication requests. If unspecified, the port number defaults to 1645.


Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use this command to add a RADIUS server to a group of RADIUS servers to be used for AAA authentication. Use the **radius-server host** command to define a RADIUS server for use by the storage router.

During authentication, the servers are accessed in the order in which they are added to the group.



Note

Verification of IP addresses in a server group occurs only at runtime. If a RADIUS server group contains an IP address that is not defined as a RADIUS server, the authentication process generates error messages and the IP address is skipped. This could cause unexpected authentication failures.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa group server radius server** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Examples

The following example identifies the servers with IP address *10.5.0.53* and *10.6.0.61* as RADIUS servers, using the default port for authentication. It creates a RADIUS server group named *region2* and adds the previously configured RADIUS servers to the *region2* group.

```
[SN5428-2A] # radius-server host 10.5.0.53
[SN5428-2A] # radius-server host 10.6.0.61
[SN5428-2A] # aaa group server radius region2
[SN5428-2A] # aaa group server radius region2 server 10.5.0.53
[SN5428-2A] # aaa group server radius region2 server 10.6.0.61
```

The following example removes the RADIUS server with IP address *10.5.0.53* from the RADIUS server group named *region2*:

```
[SN5428-2A] # no aaa group server radius region2 server 10.5.0.53
```

Related Commands

Command	Description
aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
aaa group server radius deadline	Specify the length of time the storage router can skip a RADIUS server in the named group that is marked as unavailable.
aaa test authentication	Enable testing of the specified AAA authentication list.
radius-server deadline	Specify the length of time the storage router can skip a RADIUS server that is marked as unavailable.
radius-server host	Configure remote RADIUS servers for AAA authentication services.
radius-server key	Sets the global authentication and encryption key for all RADIUS communications between the storage router and the RADIUS daemon.
radius-server retransmit	Specifies how many times the storage router resends the RADIUS request to a server before giving up.
radius-server timeout	Sets the interval the storage router waits for a RADIUS server to reply before retransmitting.
restore aaa	Restore AAA authentication services from the named configuration file.
save aaa	Save the current AAA configuration information.
scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
show aaa	Display AAA configuration information.

aaa group server tacacs+

To create a named group of TACACS+ servers to be used for AAA authentication, use the **aaa group server tacacs+** command. To disable an existing group of TACACS+ servers, use the **no** form of this command.

```
aaa group server tacacs+ name
no aaa group server tacacs+ name
```

Syntax Description	<i>name</i>	The name of the group of TACACS+ servers to be used for AAA authentication. Enter a maximum of 31 characters.
--------------------	-------------	---

Defaults	None. All configured TACACS+ servers belong to the group named <i>tacacs+</i> .	
----------	---	--

Command Modes	Administrator.	
---------------	----------------	--

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Use this command to create a subset of TACACS+ servers to be used for AAA authentication. The named group can then be added to a AAA authentication methods list, allowing the specified set of TACACS+ servers to be used for authentication. After creating the named group, use the **aaa group server tacacs+ server** command to add a TACACS+ server to the group.

Use the **tacacs-server host** command to configure a TACACS+ server to be used by the storage router for AAA authentication.

Group names must be unique across the storage router; you cannot have a group of TACACS+ servers named *labauth* and a group of RADIUS servers named *labauth*. The default group name of *tacacs+* includes all configured TACACS+ servers.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa group server tacacs+** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Examples

The following example creates a TACACS+ server group named *region3*:

```
[SN5428-2A] # aaa group server tacacs+ region3
```


Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
	aaa group server tacacs+ server	Add the specified TACACS+ server to the named TACACS+ server group.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.
	tacacs-server key	Sets the global authentication and encryption key for all TACACS+ communications between the storage router and the TACACS+ daemon.
	tacacs-server timeout	Sets the interval the storage router waits for a TACACS+ server to reply.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.

aaa group server tacacs+ server

To add a TACACS+ server to a named group of TACACS+ servers to be used for AAA authentication, use the **aaa group server tacacs+ server** command. To remove a RADIUS server from an existing group of TACACS+ servers, use the **no** form of this command.

```
aaa group server tacacs+ name server ip-address [auth-port port-number]

no aaa group server tacacs+ name server ip-address [auth-port port-number]
```

Syntax Description	<i>name</i>	The name of the group of TACACS+ servers. Enter a maximum of 31 characters.
	<i>ip-address</i>	The IP address of the TACACS+ server.
	auth-port <i>port-number</i>	(Optional) The server port number. Valid port numbers range from 1 to 65535. If unspecified, the port number defaults to 49.


Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use this command to add a TACACS+ server to a group of TACACS+ servers to be used for AAA authentication. Use the **tacacs-server host** command to define a TACACS+ server for use by the storage router.

During authentication, the servers are accessed in the order in which they are added to the group.


Note

Verification of IP addresses in a server group occurs only at runtime. If a TACACS+ server group contains an IP address that is not defined as a TACACS+ server, the authentication process generates error messages and the IP address is skipped. This could cause unexpected authentication failures.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa group server tacacs+ server** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Examples

The following example identifies the servers with IP address *172.29.39.46* and *10.7.0.72* as TACACS+ servers, using the default port for authentication. It creates a TACACS+ server group named *region3* and adds the previously configured TACACS+ servers to the *region3* group.

```
[SN5428-2A] # tacacs-server host 172.29.39.46
[SN5428-2A] # tacacs-server host 10.7.0.72
[SN5428-2A] # aaa group server tacacs+ region3
[SN5428-2A] # aaa group server tacacs+ region3 server 172.29.39.46
[SN5428-2A] # aaa group server tacacs+ region3 server 10.7.0.72
```

The following example removes the TACACS+ server with IP address *10.7.0.72* from the TACACS+ server group named *region3*:

```
[SN5428-2A] # no aaa group server tacacs+ region3 server 10.7.0.72
```

Related Commands

Command	Description
aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
aaa test authentication	Enable testing of the specified AAA authentication list.
tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.
tacacs-server key	Sets the global authentication and encryption key for all TACACS+ communications between the storage router and the TACACS+ daemon.
tacacs-server timeout	Sets the interval the storage router waits for a TACACS+ server to reply.
restore aaa	Restore AAA authentication services from the named configuration file.
save aaa	Save the current AAA configuration information.
scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
show aaa	Display AAA configuration information.

aaa new-model

To enable the AAA access control model, issue the **aaa new-model** command.

```
aaa new-model

no aaa new-model
```

Syntax Description

This command has no arguments or keywords.

Defaults

AAA is enabled. AAA cannot be disabled on the SN 5428-2 Storage Router.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

This command enables the AAA access control model. The **no aaa new-model** command is available for completeness only; AAA cannot be disabled for the storage router.

AAA authentication services are used to provide the following authentication types:

- iSCSI authentication—provides authentication of IP hosts requiring access to storage via SCSI routing instances
- Login authentication—provides authentication of users requiring Monitor mode access to the storage router via the CLI
- Enable authentication—provides authentication of users requiring Administrator mode access to the storage router via the CLI **enable** command

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa new-model** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Examples

The following example initializes AAA:

```
[SN5428-2A] # aaa new-model
```


Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
	aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
	aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	debug aaa	Enable debugging for the AAA authentication services.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

aaa test authentication

To test authentication using the specified authentication list, use the **aaa test authentication** command.

aaa test authentication {enable | login} default *username password*

aaa test authentication iscsi {listname | default} *username password*

aaa test authentication cancel

Syntax Description	enable default	Use the services in the Enable authentication list for testing. The name of the list must be <i>default</i> .
	login default	Use the services in the Login authentication list for testing. The name of the list must be <i>default</i> .
	iscsi listname	Use the services in the named iSCSI authentication list for testing.
	iscsi default	Use the services in the iSCSI authentication list for testing. The name of the list must be <i>default</i> .
	<i>username</i>	The user name to be tested.
	<i>password</i>	The password associated with the specified user name.
	cancel	Cancel any outstanding test authentication requests.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

AAA uses the services in the specified authentication list to perform Enable, Login or iSCSI authentication. Use this command to test iSCSI authentication prior to enabling authentication for SCSI routing instances or for troubleshooting purposes.

Use the **cancel** keyword to terminate any outstanding test authentication requests. For example, if a RADIUS or TACACS+ server is configured with a very long timeout value, you can cancel the request rather than waiting for the timeout to occur.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa test authentication** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Examples

The following example tests iSCSI authentication using the default authentication list for the user named *user1*, with a password of *password1*:

```
[SN5428-2A] # aaa test authentication iscsi default user1 password1
```

The following example tests iSCSI authentication using the authentication list named *webtest1*, for the user named *user2*, with a password of *password2*:

```
[SN5428-2A] # aaa test authentication iscsi webtest1 user2 password2
```

The following example tests Enable authentication for the user named *\$enab15\$*, with a password of *admin*:

```
[SN5428-2A] # aaa test authentication enable default $enab15$ admin
```

The following example tests Login authentication for the user named *monitor*, with a password of *cisco*:

```
[SN5428-2A] # aaa test authentication login default monitor cisco
```

Related Commands

Command	Description
aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
debug aaa	Enable debugging for the AAA authentication services.
radius-server host	Configure remote RADIUS servers for AAA authentication services.
restore aaa	Restore AAA authentication services from the named configuration file.
save aaa	Save current AAA configuration information.
scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
show aaa	Display AAA configuration information.
tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

accesslist

To create an access list entity, use the **accesslist** command.

accesslist *name*

Syntax Description	<i>name</i>	The name of the access list entity created by this command. Enter a maximum of 31 characters.
---------------------------	-------------	---

Defaults	None.
-----------------	-------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Access lists identify the IP hosts allowed to access a common set of storage resources and are associated with specific storage targets. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.

There is a maximum of 100 access lists per storage router or per storage router cluster. There is a maximum of 200 access list identification entries across all access lists in the storage router or storage router cluster.



Note

If there is a CHAP user name entry in the access list, the SCSI routing instance used to access the storage target must also have iSCSI authentication enabled. See [Chapter 9, “Configuring Authentication”](#) for more information about AAA and iSCSI authentication.

In a cluster environment, access list management functions are handled by a single storage router. To determine which storage router is performing access list management functions, issue the **show cluster** command. If you issue an **accesslist** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about operating the storage router in a cluster.

Examples

The following command creates an access list named *webserver2*:

```
[SN5428-2A] # accesslist webserver2
```

Related Commands

Command	Description
accesslist A.B.C.D/bits	Add IP addresses to an access list.
accesslist chap-username	Add CHAP user name entries to an access list.
accesslist description	Add a description to an access list.
accesslist iscsi-name	Add iSCSI Name entries to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

accesslist A.B.C.D/bits

To add the IP address and subnet mask of IP hosts to the named access list, use the **accesslist A.B.C.D/bits** command.

```
accesslist name A.B.C.D/bits | A.B.C.D/1.2.3.4 [A.B.C.D/bits | A.B.C.D/1.2.3.4] . . .  
[A.B.D.F/bits | A.B.C.D/1.2.3.4]
```

Syntax Description	<i>name</i>	The name of an access list to which you are adding information.
	<i>A.B.C.D/bits</i>	IP address and subnet mask of the IP host being added to the access list. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style.
	<i>A.B.C.D/1.2.3.4</i>	The IP address and subnet mask of the IP host being added to the access list. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Use the **accesslist A.B.C.D/bits** command after creating an access list to populate the list with IP address entries. Enter multiple addresses and masks, separating each by a space.

Access lists identify the IP hosts allowed to access a common set of storage resources and are associated with specific storage targets. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.

There is a maximum of 100 access lists per storage router or per storage router cluster. There is a maximum of 200 access list identification entries across all access lists in the storage router or storage router cluster.

In a cluster environment, access list management functions are handled by a single storage router. To determine which storage router is performing access list management functions, issue the **show cluster** command. If you issue an **accesslist A.B.C.D/bits** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about operating the storage router in a cluster.

Examples

The following commands add the specified entries to the named access lists:

```
[SN5428-2A] # accesslist myAccessList 192.168.54.12/32 192.168.54.15/32
* [SN5428-2A] # accesslist Webserver5 209.165.201.1/255.255.255.0
209.165.201.5/255.255.255.0
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist chap-username	Add CHAP user name entries to an access list.
accesslist description	Add a description to an access list.
accesslist iscsi-name	Add iSCSI Name entries to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

accesslist chap-username

To add the CHAP user name of IP hosts to the named access list, use the **accesslist chap-username** command.

```
accesslist name chap-username username
```

Syntax Description	<i>name</i>	The name of an access list to which you are adding information.
	<i>username</i>	The CHAP user name (used for iSCSI authentication purposes) configured for the IP host that requires access to storage.

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use the **accesslist chap-username** command after creating an access list to populate the list with CHAP user name entries. A CHAP user name is required for iSCSI authentication.

Access lists identify the IP hosts allowed to access a common set of storage resources and are associated with specific storage targets. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.

There is a maximum of 100 access lists per storage router or per storage router cluster. There is a maximum of 200 access list identification entries across all access lists in the storage router or storage router cluster.

The iSCSI driver is configured with a CHAP user name and password when SCSI routing instances have iSCSI authentication enabled. AAA authentication services authenticate the IP host using the CHAP user name and password. An access list can also use the CHAP user name to identify IP hosts allowed access to a common set of storage resources.

**Note**

If there is a CHAP user name entry in the access list, the SCSI routing instance used to access the storage target must also have iSCSI authentication enabled. See [Chapter 9, “Configuring Authentication”](#) for more information about AAA and iSCSI authentication.

In a cluster environment, access list management functions are handled by a single storage router. To determine which storage router is performing access list management functions, issue the **show cluster** command. If you issue an **accesslist chap-username** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about operating the storage router in a cluster.

Examples

The following commands add the specified entries to the named access lists:

```
[SN5428-2A] # accesslist myAccessList chap-username foo
*[SN5428-2A] # accesslist Webserver5 chap-username server1
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
accesslist description	Add a description to an access list.
accesslist iscsi-name	Add iSCSI Names to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

accesslist description

To add a description to an existing access list entity, use the **accesslist description** command.

accesslist *name* **description** “*text*”

Syntax Description	<i>name</i>	The name of an existing access list entity.
	<i>text</i>	User-defined identification information associated with this access list. Enclose the description string in quotes. Enter a maximum of 64 characters.

Defaults	None.
-----------------	-------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Access lists identify the IP hosts allowed to access a common set of storage resources and are associated with specific storage targets. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.

There is a maximum of 100 access lists per storage router or per storage router cluster. There is a maximum of 200 access list identification entries across all access lists in the storage router or storage router cluster.

In a cluster environment, access list management functions are handled by a single storage router. To determine which storage router is performing access list management functions, issue the **show cluster** command. If you issue an **accesslist description** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about operating the storage router in a cluster.

Examples

The following command adds a description to the access list named *webserver2*:

```
[SN5428-2A] # accesslist webserver2 description "Access list for company web servers"
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
accesslist chap-username	Add CHAP user name entries to an access list.
accesslist iscsi-name	Add iSCSI Name entries to an access list.
delete accesslist	Delete a specific access list entry, or an entire access list.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

accesslist iscsi-name

To add the iSCSI Name of IP hosts to the named access list, use the **accesslist iscsi-name** command.

```
accesslist name iscsi-name string
```

Syntax Description	name	The name of an access list to which you are adding information.
	string	The iSCSI Name of IP host that requires access to storage. The iSCSI Name is a UTF-8 character string based on iSCSI functional requirements. It is a location-independent permanent identifier for an iSCSI node. An iSCSI node can be either an initiator, a target, or both.

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use the **accesslist iscsi-name** command after creating an access list to populate the list with iSCSI Name entries.

If you do not know the iSCSI Name of the IP host, configure the IP host and attempt to access the desired storage targets. Use the **show scsirouter** command with the **host table** keywords to then display the iSCSI Name (along with the initiator alias, IP address and CHAP user name) of all IP hosts that have attempted to access storage resources.

Access lists identify the IP hosts allowed to access a common set of storage resources and are associated with specific storage targets. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.

There is a maximum of 100 access lists per storage router or per storage router cluster. There is a maximum of 200 access list identification entries across all access lists in the storage router or storage router cluster.

In a cluster environment, access list management functions are handled by a single storage router. To determine which storage router is performing access list management functions, issue the **show cluster** command. If you issue an **accesslist iscsi-name** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about operating the storage router in a cluster.

Examples

The following command add the specified iSCSI Name to the access list named *foo*:

```
[SN5428-2A] # accesslist foo iscsi-name ign.1987-05.com.cisco.01.88e8b25a6bf3372a34567123f
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
accesslist chap-username	Add CHAP user name entries to an access list.
accesslist description	Add a description to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

admin contactinfo

To provide basic contact information for the system administrator of this SN 5428-2 Storage Router, use the **admin contactinfo** command.

```
admin contactinfo [name "string" | email "string" | phone "string" | pager "string"]

admin contact info name "string" email "string" phone "string" pager "string"
```

Syntax Description	name <i>string</i>	(Optional) The name of the storage router administrator.
	email <i>string</i>	(Optional) The e-mail address of the storage router administrator. This is an address to which alerts may be sent.
	phone <i>string</i>	(Optional) The phone number of the storage router administrator.
	pager <i>string</i>	(Optional) The pager number of the storage router administrator.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Use the **admin contactinfo** command to provide site-specific information for the system administrator of the SN 5428-2 Storage Router. The command accepts each parameter separately, or all parameters together. If all parameters are specified, they must be in the sequence shown. Usage is completely site-specific.

Enclose each string containing spaces in single or double quotes. If a string contains a single quote, enclose it is double quotes; if it contains a double quote, enclose it in single quotes. A string cannot contain both single and double quotes.

Examples

The following commands set the system administrator name and e-mail address:

```
[SN5428-2A]# admin contactinfo name "Pat Hurley"
[SN5428-2A]# admin contactinfo email "hurley@abc123z.com"
```

The following command sets all system administrator contact information:

```
[SN5428-2A]# admin contactinfo name "Chris Smith" email "chris.smith@zxy478x.com" phone
"123.555.5555 ext 97" pager "555.3444 pin 2234"
```


Related Commands	Command	Description
	admin password	Set the login password for administrative access to the storage router management interface.
	restore system	Restore selected system information from the named configuration file.
	save all	Save all configuration information, including the system administrator contact information.
	save system	Save selected system configuration information, including the system administrator contact information.
	show admin	Display system administrator contact information.

admin password

To set the password used for administrative access to the SN 5428-2 Storage Router management interface, use the **admin password** command. Access may be via Telnet or SSH (for CLI), or web-based GUI.

admin password *string*

Syntax Description	<i>string</i>	The password associated with administrative access to the storage router management interface. The string can be enclosed in quotes, and must be enclosed in quotes if the password includes one or more spaces. A string value of "" clears the password. The default password is <i>cisco</i> .
--------------------	---------------	---

Defaults	The default password is <i>cisco</i> .
----------	--

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

The management interface is password protected. You must enter passwords when accessing the storage router via Telnet or SSH (for CLI) or web-based GUI. The Monitor mode password provides view-only access to the management interface, while the Administrator mode password allows you to create entities and make changes to the configuration of the storage router. Password protection can also be extended to the storage router console, using the **restrict console** command.

The password can contain one or more spaces, if the password string is enclosed in quotes. A string value of "" clears the password, effectively setting it to nothing.

In a cluster environment, the Administrator mode and Monitor mode passwords are cluster-wide configuration elements and apply to all storage routers in a cluster. The password management functions are handled by a single storage router. To determine which storage router is performing password management functions, issue the **show cluster** command. If you issue the **admin password** command from a storage router that is not performing password management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.


Note

The password is displayed in clear text as the command is entered, but it is changed to a series of number signs (#####) when the change is acknowledged.

Examples

The following example sets the Administrator mode password to *foo73G*. All passwords are case sensitive.

```
[SN5428-2A] # admin password foo73G
```


The following example sets the Administrator mode password to “xZm! 673”:

```
[SN5428-2A] # admin password "xZm! 673"
```

Related Commands	Command	Description
	aaa generate password	Generate a long random password.
	enable	Enter Administrator mode.
	exit	Leave Administrator mode and enter Monitor mode.
	monitor password	Set the login password for view-only access to the storage router management interface.
	restrict console	Enable or disable password checking on the storage router console interface.
	save all	Save all configuration information, including the administrator password.
	save system	Save selected system configuration information, including the Administrator mode passwords.
	setup access	Run the wizard to configure Monitor mode and Administrator mode passwords.

cdp enable

To enable Cisco Discovery Protocol (CDP) on the SN 5428-2 Storage Router, use the **cdp enable** command. To disable CDP on the storage router, use the **no** form of this command.

cdp enable

no cdp enable

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	CDP is enabled.
-----------------	-----------------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	CDP is enabled by default in order to send or receive CDP information. CDP can be switched on or off for each specific interface via the cdp interface command.
-------------------------	--

Examples	The following example enables CDP on the storage router:
-----------------	--

```
[SN5428-2A] # cdp enable
```

Related Commands	Command	Description
	cdp holdtime	Specify the amount of time the receiving device should hold a CDP packet from the SN 5428-2 Storage Router before discarding it.
	cdp interface	Switch CDP on or off for the specified interface.
	cdp timer	Specify the amount of time between transmissions of CDP packets from the SN 5428-2 Storage Router.

cdp holdtime

To specify the amount of time the receiving device should hold a CDP packet from the SN 5428-2 Storage Router before discarding it, use the **cdp holdtime** command. To revert to the default setting, use the **no** form of this command.

cdp holdtime *nn*

no cdp holdtime

Syntax Description

<i>nn</i>	The holdtime to be sent in the CDP update packets, in seconds.
-----------	--

Defaults

The default holdtime is 180 seconds.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The CDP holdtime must be set to a higher number of seconds than the time between CDP transmissions, which is set using the **cdp timer** command.

Examples

The following example sets the CDP holdtime to 60, meaning that the CDP packet being sent from the storage router should be held by the receiving device for 60 seconds before being discarded. You may want to set the holdtime lower than the default setting of 180 seconds if information about the storage router changes frequently.

```
[SN5428-2A] # cdp holdtime 60
```

Related Commands

Command	Description
cdp enable	Enable or disable CDP on the SN 5428-2 Storage Router.
cdp interface	Switch CDP on or off for the specified interface.
cdp timer	Specify the amount of time between transmissions of CDP packets from the SN 5428-2 Storage Router.

cdp interface

To enable CDP for a specific interface, use the **cdp interface** command. To disable CDP for a specific interface, use the **no** form of this command.

cdp interface *if-name* **enable**

no cdp interface *if-name* **enable**

Syntax Description	<i>if-name</i>	The name of the interface for which you are enabling or disabling CDP. CDP can be enabled on the management (mgmt), HA, and Gigabit Ethernet (ge2) interfaces. When you type the cdp interface ? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
	enable	Keyword used to enable CDP for the specified interface.

Defaults	CDP is enabled for all interfaces.
----------	------------------------------------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	CDP must be enabled for the SN 5428-2 Storage Router, using the cdp enable command, before it can be enabled for a specific interface.
------------------	---

Examples	The following example enables CDP for the Gigabit Ethernet interface, <i>ge2</i> :
----------	--

[SN5428-2A] # **cdp interface ge2 enable**

The following example disables CDP for the management interface:

[SN5428-2A] # **no cdp interface mgmt enable**

Related Commands	Command	Description
	cdp enable	Enable or disable CDP on the SN 5428-2 Storage Router.
	cdp holdtime	Specify the amount of time the receiving device should hold a CDP packet from the SN 5428-2 Storage Router before discarding it.
	cdp timer	Specify the amount of time between transmissions of CDP packets from the SN 5428-2 Storage Router.

cdp timer

To specify the amount of time between transmissions of CDP packets from the SN 5428-2 Storage Router, use the **cdp timer** command. To revert to the default setting, use the **no** form of this command.

cdp timer *nn*

no cdp timer

Syntax Description

<i>nn</i>	The number of seconds between transmissions of CDP packets from the SN 5428-2 Storage Router.
-----------	---

Defaults

The default is 60 seconds.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The time between CDP transmissions must be set to a lower number than the CDP holdtime, which is set using the **cdp holdtime** command. There is a trade-off between sending more frequent CDP updates and bandwidth utilization.

Examples

The following example sets the CDP timer to 90, meaning that CDP updates are sent every 90 seconds, which is less frequently than the default of 60 seconds. You may want to make this change if you are concerned about preserving bandwidth.

```
[SN5428-2A] # cdp timer 90
```

Related Commands

Command	Description
cdp enable	Enable or disable CDP on the SN 5428-2 Storage Router.
cdp holdtime	Specify the amount of time the receiving device should hold a CDP packet from the SN 5428-2 Storage Router before discarding it.
cdp interface	Switch CDP on or off for the specified interface.

clear conf

To return certain configuration settings to factory defaults, use the **clear conf** wizard. The **clear conf** wizard prompts you to enter the Administrator mode password and then to indicate which settings to restore to factory defaults.

clear conf

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines The **clear conf** wizard is only available when the storage router is deployed for SCSI routing. If the storage router is deployed for transparent SCSI routing, use the **clear conf {all | system}** command to return the storage router configuration to factory default settings.

Follow these guidelines when using the **clear conf** wizard:

- Select **apps** to remove all SCSI routing instances but retain system configuration settings.
- Select **system** to remove all SCSI routing instances and system configuration settings.
- Select **saved** to delete all backup configuration files from disk.
- Select **all** to remove all SCSI routing instances, system configuration settings, and saved configuration files.

The system will reboot if you select **apps**, **system**, or **all**.

System configuration settings include:

- The management and HA interface IP addresses
- Configuration information for Fibre Channel interfaces
- Saved zone configuration information
- Domain name servers
- NTP server and time zone information
- SNMP information
- Administrator and Monitor passwords, and administrator contact information
- AAA authentication configuration information
- VLAN and VTP information

Deleting system configuration makes the storage router unavailable to Telnet, SSH or web-based GUI sessions until the management interface is reconfigured with an IP address via a console connection. See [Chapter 2, “First-Time Configuration,”](#) for more information about initial system configuration.

**Note**

The **clear conf** wizard will not reset any Secure Shell (SSH) public and private key pairs generated for the storage router. Use the **ssh keygen** command to generate new SSH keys after the storage router is restored to the selected factory default settings.

Examples

The following example removes all SCSI routing instances from the storage router. The system configuration settings are retained.

```
[SN5428-2_A1]# clear conf
```

```
Enter admin password: *****
```

```
This process can restore factory default settings for the SN5428-2.
```

- * Select "apps" to remove active applications and retain system configuration settings.
- * Select "system" to remove active applications and system configuration settings.
- * Select "saved" to remove all backup configurations from disk.
- * Select "all" to remove active applications, system configuration, and saved configurations.

```
The system configuration includes the management port, dns, admin and monitor login, ntp, and snmp. You will need to use the console to reconfigure the management port if you erase the system configuration.
```

```
The system will reboot if you select "apps", "system", or "all".
```

```
Erase what? [apps/system/saved/all/cancel (cancel)]apps
```

```
Configuration cleared. System configuration settings retained.
System halting.....!
```

```
System has been halted
```

Related Commands

Command	Description
setup access	Run the wizard to configure Monitor mode and Administrator mode passwords.
setup cluster	Change the configuration of the high availability environment.
setup fcip	Run the wizard to manually configure FCIP instances.
setup iscsi-port	Run the wizard to manually configure the port used for iSCSI traffic.
setup mgmt	Run the wizard to configure the management interface.
setup netmgmt	Run the wizard to configure network management.
setup scsi	Run the wizard to configure a SCSI routing instance.
setup time	Run the wizard to configure the system date and time.

clear conf {all | system}

To return certain configuration settings to factory defaults, use the **clear conf {all | system}** command.

clear conf {all | system} password

Syntax Description

all	Remove all storage router configuration information, including system configuration settings, saved configuration files, SCSI routing and FCIP instances, access lists, and cluster configuration settings.
system	Remove all system configuration settings, SCSI routing instances, access lists and cluster configuration settings. Saved configuration files will be retained.
<i>password</i>	The Administrator mode password.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

System configuration settings include:

- The management and HA interface IP addresses
- Configuration information for Fibre Channel interfaces
- Saved zone configuration information
- Domain name servers
- NTP server and time zone information
- SNMP information
- Administrator and Monitor passwords, and administrator contact information
- AAA authentication information
- VLAN and VTP information

Issuing the **clear conf** command with either the **system** or **all** keyword causes the storage router to reboot.

Deleting system configuration makes the storage router unavailable to Telnet or web-based GUI sessions until the management interface is reconfigured with an IP address via a console connection. See [Chapter 2, “First-Time Configuration,”](#) for more information about initial system configuration.

**Note**

The **clear conf** command will not reset any Secure Shell (SSH) public and private key pairs generated for the storage router. Use the **ssh keygen** command to generate new SSH keys after the storage router is restored to the selected factory default settings.

Examples

The following example removes all storage router configuration information, returning the storage router to its initial default configuration. The example uses the default Administrator mode password, *cisco*.

```
[SN5428-2_A1]# clear conf all cisco
```

```
Clearing configuration...
```

```
Current configuration and named configurations cleared.  
System halting.....
```

Related Commands

Command	Description
clear conf	Run the wizard to reset the storage router to factory defaults.
setup access	Run the wizard to configure Monitor mode and Administrator mode passwords.
setup cluster	Change the configuration of the storage router's high availability environment.
setup fcip	Run the wizard to manually configure FCIP instances.
setup iscsi-port	Run the wizard to manually configure the port used for iSCSI traffic.
setup mgmt	Run the wizard to configure the management interface.
setup netmgmt	Run the wizard to configure network management.
setup scsi	Run the wizard to configure a SCSI routing instance.
setup time	Run the wizard to configure the system date and time.

clear counters fcip

To clear all counters associated with the specified FCIP instance, or all instances, use the **clear counters fcip** command.

clear counters fcip {*name* | **all**}

Syntax Description

<i>name</i>	The name of the FCIP instance for which counters will be cleared.
all	Clear counters for all FCIP instances.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced.

Usage Guidelines

This command resets the specified operational statistics. It does not display the accumulated statistics before resetting the counters.

Clear counters before beginning a troubleshooting session, so you can quickly identify the counters that are changing.

Examples

The following example clears the operational counters for the FCIP instance named *fcip1*:

```
[SN5428-2A] # clear counters fcip fcip1
```

The following example clears the operational counters for all FCIP instances:

```
[SN5428-2A] # clear counters fcip all
```

Related Commands

Command	Description
fcip	Create an FCIP instance.
show fcip	Display configuration and operational information for the named FCIP instance.

clear counters interface

To clear all counters associated with the specified interface, or all interfaces, use the **clear counters interface** command.

clear counters interface {*if-name* | **all**}

Syntax Description

<i>if-name</i>	The name of the interface. Counters can be cleared for the management (mgmt), Fibre Channel (fc?), FC initiator interfaces (fci?), Gigabit Ethernet (ge?) interfaces, and the high availability (ha) interface (if available). When you type the clear counters interface ? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
all	Clear counters for all interfaces.

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

This command resets all accumulated operational statistics for the specified interface. Operational statistics can include counters for packets received and transmitted, collisions, octets, multicast packets, dropped and unsupported protocol, exception status IOCBs (such as LIP reset aborts, port unavailable or logged out, DMA errors, port configuration changed, command timeout, data overrun, write or read data underrun, and queue full), Fibre Channel errors, and other general events.

Clear counters before beginning a troubleshooting session, so you can quickly identify the counters that are changing.

Examples

The following example clears all accumulated operational statistics counters for the Fibre Channel interface *fc1*.

```
[SN5428-2A]# clear counters interface fc1
```

Related Commands

Command	Description
show interface	Display operational and configuration information for the specified interface or all interfaces.

clear counters scsirouter

To reset accumulated operational statistics for the specified SCSI routing instance, use the **clear counters scsirouter** command.

clear counters scsirouter {*name* | **all**} {**connection** | **host** | **target** {*name* | **all**}}

Syntax Description

<i>name</i>	The name of the SCSI routing instance for which counters will be cleared.
all	Clear counters for all SCSI routing instances.
connection	Clear operational statistics related to connections only.
host	Clear operational statistics related to currently connected hosts only.
target <i>name</i>	Clear operational statistics related to the specified target.
target all	Clear operational statistics related to all targets.

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

This command resets the specified operational statistics. It does not display the accumulated statistics before resetting the counters.

Clear counters before beginning a troubleshooting session, so you can quickly identify the counters that are changing.

Examples

The following example clears the connection counters for the SCSI routing instance *myScsi1*.

```
[SN5428-2A]# clear counters scsirouter myScsi1 connection
```

Related Commands

Command	Description
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

clear fcswitch

To clear the switch log files of all entries or to clear stored zoning configuration information, issue the **clear fcswitch** command.

```
clear fcswitch {devlog | syslog | zones {fabric | local}}
```

Syntax Description

devlog	The switch development log file.
syslog	The switch system log file.
zones	Zoning changes received from switches in the fabric and stored by the SN 5428-2 Storage Router.
fabric	Keyword used to clear the local zoning database and deactivate the active zone set for the entire fabric.
local	Keyword used to clear the local zoning database for the storage router only. All ports operating as E_Ports must be inactive before the local zoning configuration is cleared.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Clear the switch development or system log file if it is large, or if you are going to perform testing and want to be sure the switch log files only reflects information from the testing session.

Clear local zoning configuration if you are moving the storage router from one FC switched zoned fabric to another or removing a switch from the fabric, or when other network changes have been made that render the saved zoning information inaccurate. All ports operating as E_Ports must be inactive. If the **clear fcswitch zones local** command is issued when there is an active E_Port on the SN 5428-2 Storage Router, the command fails and issues a warning message indicating the FC interfaces that are currently enabled.

Use the **fabric** keyword to clear the local zoning database and deactivate the active zoneset for the entire fabric.

Examples

The following example clears the switch development log files:

```
[SN5428-2A] # clear fcswitch devlog
```

The following example clears the switch system log files:

```
[SN5428-2A] # clear fcswitch syslog
```


■ clear fcswitch

The following example clears all saved zoning information from the storage router local zoning database:

```
[SN5428-2A]# clear fcswitch zones local
```

The following example clears the local zoning database and deactivates the active zone set for the entire fabric:

```
[SN5428-2A]# clear fcswitch zones fabric
```

Related Commands

Command	Description
fcswitch devlog	Specify logging parameters for the switch development log file.
fcswitch domainid	Set the domain ID for the storage router, to be used for FC switched fabric zoning.
fcswitch syslog	Specify logging parameters for the switch system log file.
fcswitch zoning autosave	Configure the storage router to participate in FC switched fabric zones.
show debug fcswitch	Display internal FC interface parameters, including switch log entries.
show fcswitch	Display global configuration information for storage router FC interfaces.
show fcswitch fabric	Display information about the Fibre Channel fabric.
show fcswitch linkstate	Display information about the storage router link state database.
zone	Create a Fibre Channel fabric zone.
zoneset	Create a Fibre Channel fabric zone set.

clear log

To clear the SN 5428-2 Storage Router log file of all entries, issue the **clear log** command.

clear log

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1.	This command was introduced.

Usage Guidelines	Clear the storage router log file if it is large, or if you are going to perform testing and want to be sure the log file only reflects information from the testing session.
-------------------------	---

Examples	The following example clears all entries from the storage router log file: [SN5428-2A] # clear log
-----------------	--

Related Commands	Command	Description
	logging level	Add rule entries to route storage router event, debug and trace messages to various destinations based on facility and notification level.
	show logging	Display the routing rules in the logging table and the contents of the storage router log file.

clear logging table

To clear the SN 5428-2 Storage Router logging table of all entries, or to reset the table to factory defaults, issue the **clear logging table** command.

clear logging table [to factory_defaults]

Syntax Description	to factory_defaults Return the storage router logging table to the factory default logging rule entries.	
Defaults	None.	
Command Modes	Administrator.	
Command History	Release	Modification
	3.2.1.	This command was introduced.
Usage Guidelines	<p>Use this command to remove all rules for routing storage router event messages. If the logging table is cleared, logging is still enabled but all messages will be discarded.</p> <p>To return the logging table to the factory default logging rules, use the to factory_defaults keywords. The factory default logging rules are as follows:</p> <ul style="list-style-type: none"> All messages from all facilities at notice level or lower levels are logged to all destinations. All messages from all facilities at info level or lower levels are logged to the storage router log file. 	
Examples	<p>The following example clears all entries from the storage router logging table and returns the table to the default logging rules:</p> <pre>[SN5428-2A] # clear logging table to factory_defaults</pre>	
Related Commands	Command	Description
	delete logging	Delete a rule from the logging table.
	logging #?	Insert a routing rule entry into the storage router logging table.
	logging level	Add rule entries to route storage router event, debug and trace messages to various destinations based on facility and notification level.
	logging on	Enable or temporarily disable logging of storage router event message.
	show logging	Display the routing rules in the logging table and the contents of the storage router log file.

clear scsirouter failover

To clear the primary or secondary storage router from the HA failover list for the specified SCSI routing instance, use the **clear scsirouter** command.

clear scsirouter *name* **failover** {**primary** | **secondary**}

Syntax Description

<i>name</i>	The name of the SCSI routing instance.
primary	Delete the current primary storage router from the HA failover list.
secondary	Delete the secondary storage router from the HA failover list.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use the **clear scsirouter failover** command to reset the primary or secondary storage router on the HA failover list for the specified SCSI routing instance. If there is no primary or secondary storage router configured on the HA failover list when the SCSI routing instance fails over, the cluster attempts to run the instance on the first node that is available based on HA failover eligibility information.

Use the **scsirouter failover** command to add a storage router to the HA failover list.



Note

This command causes the SCSI routing instance configuration information to be saved and all nodes in the cluster to be updated.

Examples

The following example removes the current primary storage router from the HA failover list for SCSI routing instance *foo*:

```
[SN5428-2A]# clear scsirouter foo failover primary
```


Related Commands	Command	Description
	failover scsirouter	Cause the named SCSI routing instance to cease running on the storage router.
	scsirouter failover	Add the storage router to the HA failover list for the specified SCSI routing instance.

clear scsirouter primary

To remove the storage router configured as the primary for the named SCSI routing instance, use the **clear scsirouter primary** command.

clear scsirouter *name* **primary**

Syntax Description	<i>name</i>	The name of the SCSI routing instance.
--------------------	-------------	--

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	<p>At any given time, a SCSI routing instance can run on only one storage router in a cluster. If a SCSI routing instance has the primary attribute set, the specified storage router will take over running that instance upon system restart or whenever target and critical resources are available.</p> <p>If the primary attribute is not set, the SCSI routing instance continues running on the node where it was started until it is explicitly stopped (via a no scsirouter enable command), it automatically fails over to another storage router in the cluster because targets or critical resources are unavailable, or an explicit failover scsirouter command is issued. This is the default behavior.</p>
------------------	---

Examples	<p>The following command removes the storage router configured as the primary for the SCSI routing instance named lab2:</p>
----------	---

```
[SN5428-2A] # clear scsirouter lab2 primary
```

Related Commands	Command	Description
	clear scsirouter failover	Remove the designated primary or secondary storage router from the HA failover list for the specified SCSI routing instance.
	scsirouter primary	Identify the storage router as the preferred storage router to run the named SCSI routing instance.
	scsirouter failover	Add the storage router to the HA failover list for the specified SCSI routing instance.

clear static

To clear the mapping of the IP host to Fibre Channel (FC) address for the specified World Wide Port Name (WWPN), use the **clear static** command. This command is only available when the storage router is deployed for static transparent SCSI routing.

clear static iscsibindings {all | xxxxxxxxxxxxxxxx}

Syntax Description	iscsibindings all	Clear all IP host to FC address mappings.
	iscsibindings xxxxxxxxxxxxxxxx	Clear the mapping represented by this WWPN.
	Note	WWPN address notation is represented by 16 hex digits. The digits may be separated by colons. When using WWPN addresses in this command, colons can be omitted or placed anywhere in the address notation as long as they do not leave one character without a partner character.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.3.1	This command was introduced.

Usage Guidelines

When the storage router is deployed for static transparent SCSI routing, the IP host to FC address mappings are saved and retained in the storage router when it is restarted. If an IP host will no longer be accessing storage via the SN 5428-2, or if you want the SN 5428-2 to create a new mapping when the IP host logs in again, you can clear an existing mapping. Mappings can only be cleared if they are not currently in use.

To display the mappings that are currently configured in the storage router, use the **show static iscsibindings** command.

Examples

The following example displays the currently configured mappings, and then deletes the mapping for the IP host at IP address 10.1.20.2 (WWPN 280100065338d6c0):

```
[SN5428-2A]# show static iscsibindings
Interface WWPN                Host IP Address  Host Name
-----
fci1      280100065338d6c0  10.1.20.2       iscsi.cisco.testlab
fci1      280200065338d6c0  10.1.4.213      iqn.1987-05.com.cisco.02.0AB08....B6E5CCE.WIN1
fci2      290100065338d6c0  10.1.30.100     iqn.1987-05.com.cisco.02.9FD389....36D3D3.NT10

[SN5428-2A]# clear static iscsibindings 280100065338d6c0
Binding cleared for WWPN 280100065338d6c0
```


The following example clears all IP host to FC mappings saved in the storage router. If a mapping is in use by an IP host, the mapping will not be cleared.

```
[SN5428-2A] # clear static iscsibindings all
```

Related Commands

Command	Description
show static	Display the currently configured IP host to FC address mappings saved in the storage router.

clock set

To set the storage router system clock to the given date and time, use the **clock set** command. Date and time information is used for log files and the user interface.

clock set *hh:mm:ss mm dd yyyy*

Syntax Description

<i>hh:mm:ss mm dd yyyy</i>	The current time in hours, minutes, and seconds, followed by the current month, day, and year. For example, 13:55:22 06 22 2001.
----------------------------	--

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

If the storage router should synchronize its date and time with a network time protocol (NTP) server, see the **ntp peer** command.

Examples

The following example sets the storage router date and time to June 22, 2001 at 14:39:00.

```
[SN5428-2A] # clock set 14:39:00 06 22 2001
```

Related Commands

Command	Description
clock timezone	Specify the time zone for the storage router.
ntp peer	Specify the name or IP address of the NTP server with which the storage router will synchronize date and time.
setup time	Run the wizard to configure the system date and time.
show clock	Display the current system date and time, including the system timezone.

clock timezone

To specify the time zone for the storage router, use the **clock timezone** command.

clock timezone {*string* | ?}

Syntax Description	<i>string</i>	A character string representing the time zone of the storage router. For example, <i>America/Chicago</i> or <i>Europe/Amsterdam</i> .
	?	Display a list of all valid time zones. Use any time zone in this list for the <i>string</i> parameter to set the storage router to that time zone.

Defaults	None.
-----------------	-------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Unless you specify the time zone, the clock setting is assumed to be in Universal time, also known as Greenwich Mean Time (GMT).
	You can use the setup time wizard to select a time zone, set the clock and date, and identify an NTP server for the storage router.
	To use the clock timezone command, you must know the appropriate time zone string. Use the “?” to display a list of valid time zone strings.

Examples	The following example sets the storage router time zone to US/Mountain:
	<pre>[SN5428-2A]# clock timezone US/Mountain</pre>

Related Commands	Command	Description
	clock set	Set the storage router system clock.
	ntp peer	Specify the name or IP address of the NTP server with which the storage router will synchronize date and time.
	setup time	Run the wizard to configure the system date and time.
	show clock	Display the current system date and time, including the system time zone.

copy

To copy the named configuration file or script file from the specified location to the *savedconfig* or *script* directory, or from the storage router to the specified location, use the **copy** command. The exchange is via HTTP or TFTP. When copying files to the storage router, any file of the same name in the *savedconfig* or *script* directory is overwritten.

copy **http://***FileUrl* {**savedconfig:***configfilename* | **script:***scriptfilename*}

copy **tftp://***Location/Directory/Filename* {**savedconfig:***configfilename* | **script:***scriptfilename*}

copy {**savedconfig:***configfilename* | **script:***scriptfilename*} **tftp://***Location/Directory/Filename*

Syntax Description	<p><i>FileUrl</i></p> <p>The URL (including the file name) of the configuration or script file to be copied to the storage router, such as <i>http://acme/~myhome/allconf.xml</i>. (In this example, the host name <i>acme</i> can be used if the ip name-server command was previously issued.) Configuration files are transferred to the <i>savedconfig</i> directory; script files are transferred to the <i>script</i> directory.</p>
	<p><i>configfilename</i></p> <p>The name of the saved configuration file. If the file is being copied from the storage router to a TFTP server, it must exist in the storage router <i>savedconfig</i> directory.</p>
	<p><i>scriptfilename</i></p> <p>The name of the saved script file. If the file is being copied from the storage router to a TFTP server, it must exist in the storage router <i>script</i> directory.</p>
	<p><i>Location/Directory/File name</i></p> <p>The name of the TFTP server and default directory, followed by the file name. The file must currently exist in the directory. It will be overwritten by the file copied from the storage router.</p> <p>Note If the default directory is <i>tftpboot</i>, specify only the name of the TFTP server and the file name.</p>

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines The **copy** command does not affect the running or persistent configuration of the storage router or high availability cluster. However, the **restore** command can be used to copy the contents of a saved configuration file into persistent memory, while the **read script** command can be used to execute the commands in a script file to modify a storage router configuration.

Because TFTP does not require a user name and password, directories and files cannot be created. When you copy a file to a TFTP server, you must have read/write permissions for the complete file path, and the file copied from the storage router must already exist.

Examples

The following example copies the saved configuration file *myFoo.xml* from a server with an IP address of 10.1.40.10 to the storage router. The file name is changed to *myFoo_restore.xml* when it is written to the storage router *savedconfig* directory.

```
[SN5428-2A]# copy http://10.1.40.10/usr/SN5428-2/savedconfig/myFoo.xml
savedconfig:myFoo_restore.xml
```

The following example copies the script file *SN5428-2_Lab* from a server named *acme*. The file name is unchanged when it is written to the storage router *script* directory.

```
[SN5428-2A]# copy http://acme/~myhome/SN5428-2_Lab script:SN5428-2_Lab
```

The following example copies the saved configuration file, *backup_23*, to the *daily_backup* file in the *tftpboot* directory of the *tftp_primary* server. The file, *daily_backup*, must already exist in the *tftpboot* directory of the *tftp_primary* server. This command will overwrite the existing *daily_backup* file.

**Note**

Because the default directory is *tftpboot*, the command does not specify directory information.

```
[SN5428-2A]# copy savedconfig:backup_23 tftp://tftp_primary/daily_backup
```

Related Commands

Commands	Description
read script	Read and execute the CLI commands in the named script file.
restore aaa	Restore AAA authentication services from the named configuration file.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
restore all	Restore the contents of the named configuration file into memory.
restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
restore system	Restore selected system information from the named configuration file.
restore vlan	Restore VLAN configuration information from the named configuration file.
save aaa	Save the current AAA configuration information.
save accesslist	Save configuration data for the named access list or all access lists.
save all	Save all configuration information.
save scsirouter	Save configuration information for the named SCSI routing instance.
save system	Save selected system configuration information.
save vlan	Save configuration information for the named VLAN or for all VLANs.
show savedconfig	Display the contents of the <i>savedconfig</i> directory or the contents of the named configuration file.
show script	Display the contents of the <i>script</i> directory or the contents of the named command file.

debug aaa

To enable debugging for authentication, authorization, and accounting (AAA) services, use the **debug aaa** command. To disable debugging for AAA authentication services, use the **no** form of this command.

debug aaa

no debug aaa

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	Debugging is not enabled.
-----------------	---------------------------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modifications
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to debug problems with iSCSI, Enable and Login authentication or general AAA authentication services. Create log route entries for notification level <i>debugging</i> to send the trace and debug messages to the desired destination, using the logging level command.
-------------------------	--

Examples	The following example enables AAA debugging: [SN5428-2A] # debug aaa
-----------------	--

Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
	aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
	aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
	aaa test authentication	Enable testing of AAA authentication services.
	debug scsirouter	Enable debugging for the named SCSI routing instance.
	logging level	Add rule entries to route storage router event, debug and trace messages to various destinations based on facility and notification level.
	restore aaa	Restore AAA configuration services from a saved configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.

debug cmd

To run any operating system command with up to five arguments from the CLI, use the **debug cmd** command.

debug cmd *os-command* [*parameters*]

Syntax Description

<i>os-command</i>	Any valid operating system command. Do not invoke interactive functions.
<i>parameters</i>	Up to five command parameters.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modifications
3.2.1	This command was introduced.

Usage Guidelines

The **debug cmd** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

Examples

The following example displays usage information for the **debug cmd**:

```
[SN5428-2A]# debug cmd dbgRunOSCmdHelp 0
[SN5428-2A]# debug cmd dbgRunOSCmdHelp 0c 1a c4 3c

Running command dbgRunOSCmdHelp(0xc1ac43c) with args 0 0 0 0 0

CLI usage: debug cmd symbol arg1 .. arg5
symbol -- any named OS function
arg1 .. arg5 -- numbers (interpreted as hex) or
                strings if escaped with an initial '$', such as $fcl
                Anything that doesn't convert to a number is a string

Return value is 0 = 0x0 (OK)
```

Related Commands

Command	Description
debug aaa	Enable debugging for AAA authentication services.
debug scsirouter	Enable debugging for the named SCSI routing instance.

debug fcip

To enable trace facilities for debugging FCIP instances, use the **debug fcip** command. To disable debugging, use the **no** form of this command.

debug fcip *name* {**mailboxtrace** | **packettrace** *mask*}

no debug fcip *name* **mailboxtrace**

Syntax Description

<i>name</i>	The name of the FCIP instance to be debugged.
mailboxtrace	Keyword, indicating that mail box tracing services will be enabled.
packettrace <i>mask</i>	Keyword, indicating that packet tracing services will be enabled. The mask value indicates the traces to capture, in hex. The default value, 0xFFFF, captures all traces. A value of 0x0000 turns off packet tracing.

Defaults

All trace facilities are enabled, by default. The packet trace mask value defaults to 0xFFFF, capturing all traces.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced.

Usage Guidelines

The **debug fcip** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

Use this command to trace traffic associated with the named FCIP instance. Use the **show debug fcip** command to view the trace buffer output. The *mask* value defaults to 0xFFFF, all packets are traced. A *mask* value of 0x0000 will turn off packet tracing.

Debug settings are not persistent and will return to default value when the storage router is rebooted. To retain a mask value for packet tracing services, use the **fcip destination config** command with the **pktracemask** keyword to change the FCIP instance configuration and then save the changes to the storage router bootable configuration.

Examples

The following example enables the debug mail box tracing services for the FCIP instance named *fcip1*:

```
[SN5428-2A]# debug fcip fcip1 mailboxtrace
```

The following example enables the debug packet tracing services for the FCIP instance named *fcip2*. All packets will be traced.

```
[SN5428-2A]# debug fcip fcip2 packettrace 0xffff
```


The following example disables debug mail box tracing services for the FCIP instance named *fcip1*:

```
[SN5428-2A]# no debug fcip fcip1 mailboxtrace
```

The following example turns off all packet tracing services for the FCIP instance named *fcip2*:

```
[SN5428-2A]# debug fcip fcip2 packettrace 0x0000
```

Related Commands

Command	Description
fcip	Create an FCIP instance.
fcip destination config	Configure operational parameters for the named FCIP instance.
show debug fcip	Display debugging information for the named FCIP instance.

debug interface

To specify the maximum number of firmware dump files that can exist on the storage router for a specified initiator interface, or to remove all existing firmware dump files, use the **debug interface** command.

debug interface *if-name* {**forcefcfwdump** | **lldrestartfcfw**}

debug interface *if-name* **fwdumpcount** *nn*

debug interface *if-name* **removefw dumps**

Syntax Description

<i>if-name</i>	Enable IP trace for the FC initiator interfaces. When you type the debug interface ? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
forcefcfwdump	Force a dump of FC firmware. A file named <i>qlclifwdump01.txt</i> is created in the <i>/ata4</i> partition.
lldrestartfcfw	Restart the FC firmware. Any existing connections may be dropped.
fwdumpcount <i>nn</i>	Specify the maximum number of times the firmware dump files for the specified interface can be overwritten. If a firmware dump is requested and the dump files cannot be overwritten, the firmware will be restarted but a dump file will not be created. The default is 1.
removefw dumps	Keyword used to clear all existing firmware dump files for the specified interface from the storage router.

Defaults

The maximum number of times firmware dump files can be overwritten for each FC initiator interface is 1.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Best practices suggest clearing all existing firmware dump files for the specified interface before requesting a new firmware dump.



Caution

Some **debug interface** commands may perform actions that drop existing connections or otherwise impact normal storage router performance. The **debug interface** command is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.

Examples

The following example sets the maximum number of times the firmware dump files for *fci1* can be overwritten to 2:

```
[SN5428-2A] # debug interface fci1 fwdumpcount 2
```

The following example clears all firmware dump files for *fci2*:

```
[SN5428-2A] # debug interface fci2 removefwdumps
```

Related Commands

Command	Description
show debug	Display a variety of debug information or perform specific troubleshooting activities.
show interface	Display operational and configuration information for the specified interface or all interfaces.

debug interface fc?

To configure a variety of operational parameters for the internal FC interface switch ports, use the **debug interface fc?** command. To disable various parameters, use the **no** form of this command.

debug interface *fc?* {al-fairness | fan-enable | lms-enable} enable

debug interface *fc?* default

debug interface *fc?* diag

debug interface *fc?* enable

debug interface *fc?* ext-credit *nn*

debug interface *fc?* linkspeed {auto | 1gb | 2gb}

debug interface *fc?* loopback {external | internal | online}

debug interface *fc?* mfs-bundle enable [timeout *nn*]

debug interface *fc?* type {auto | donor | f-port | fl-port | g-port | gl-port}

debug interface *fc?* type tl-port mode {autobridge | autolearn}

no debug interface *fc?* {al-fairness | fan-enable | ms-enable} enable

no debug interface *fc?* enable

no debug interface *fc?* mfs-bundle enable [timeout *nn*]

Syntax Description

<i>fc?</i>	The name of the internal FC interface switch port for which you are setting this parameter. Valid values are fc0 and fc15. When you type the debug interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
al-fairness enable	Keywords, used to enable the fairness algorithm (loop priority) on the named internal switch port.
default	Keyword used to reset the port to default operational parameters.
diag	Keyword used to places the switch port into diagnostic mode for testing purposes.
enable	Keyword used to enable the specified switch port.
ext-credit <i>nn</i>	Keywords used to enable the port to use additional data buffer credits. Valid values are 0, 11, 22, 33, 44, 55, 66 and 77. The default is 0, indicating that the port is not enabled for credit extension.
fan-enable enable	Keywords, used to enable Fabric Address Notification (FAN) on the specified switch port.
linkspeed auto	Keywords, indicating that the transfer rate is negotiated.
linkspeed 1gb	Keywords, indicating the transfer rate is fixed at 1 Gbps.
linkspeed 2gb	Keywords, indicating the transfer rate is fixed at 2 Gbps.

loopback external	Keywords, indicating an external test will be performed. The specified port must be in a diagnostic state.
loopback internal	Keywords, indicating an internal test will be performed. The specified port must be in a diagnostic state.
loopback online	Keywords, indicating an online loopback test will be performed. The specified port must be enabled.
mfs-bundle enable	Keywords, used to enable Multi-Frame sequence (MFS) bundling for the named switch port.
timeout <i>nn</i>	The timeout value associated with MFS bundling, in milliseconds. Valid values are 10 through 20480. The default timeout value is 10 msecs.
ms-enable enable	Keywords, used to enable GS-3 management server commands for the specified switch port.
type auto	Keywords, indicating the port type is automatically negotiated and functions as a generic loop (GL_Port).
type donor	Keywords, indicating the port type is donor. A donor port places its data buffer credits in a pool that ports configured for credit extension draw on. A donor port is essentially disabled; it cannot be used for FC communication.
type f-port	Keywords, indicating that the port type is fabric. F_Ports are fabric ports.
type fl-port	Keywords, indicating that the port type is fabric loop (also known as “public loop”).
type g-port	Keywords, indicating that the port type is generic and can function as either an F_Port or an E_Port. An E_Port is also known as an “expansion port.”
type gl-port	Keywords, indicating that the port type is generic loop and can function as either an F_Port, FL_Port, or E_Port.
type tl-port	Keywords, indicating that the port type is translated loop.
mode autobridge	Keywords, indicating public targets are made visible to the initiator in a private loop.
mode autolearn	Keywords, indicating targets in a private loop are made visible.

Defaults

The internal FC switch ports have the following default operational characteristics:

- fairness algorithm is disabled (switch has priority)
- Fabric Address Notification (FAN) is enabled
- transfer rate is fixed at 2 Gbps
- Multi-Frame sequence bundling is enabled
- GS-3 management server commands are enabled
- port type is fabric (F_Port)
- credit extension is disabled (ext-credit is set to 0)

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The **debug interface fc?** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

**Caution**

Changing operational characteristic for the interface FC switch ports can cause unexpected behavior in the storage router.

Examples

The following example places the internal FC switch port *fc0* into diagnostic mode for testing purposes:

```
[SN5428-2A] # debug interface fc0 diag
```

Related Commands

Command	Description
show debug interface fc?	Display debug information for internal FC interface switch ports.

debug interface ge?

To enable packet tracing on a Gigabit Ethernet interface, use the **debug interface ge?** command. To disable packet tracing, use the **no** form of this command.

```
debug interface ge? trace [pktcnt nn] [pktsize nn] enable

no debug interface ge? trace enable
```

Syntax Description

ge?	Enable IP trace for the specified Gigabit Ethernet interface. When you type the debug interface ge? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
trace	Keyword indicating IP packet tracing will be enabled.
pktcnt nn	(Optional) Specify the maximum number of packets to be traced. <i>nn</i> must be a value greater than zero (0). If not specified, a circular trace buffer is used. This is the default.
pktsize nn	(Optional) Specify the maximum number of bytes to trace per packet. Valid values are 14 to 1024, inclusive. The default is 128.
enable	Keyword used to enable IP packet tracing.

Defaults

IP packet tracing for all Gigabit Ethernet interfaces is disabled by default. The maximum trace size is 128, and all packets use a circular trace buffer.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

- The **debug interface ge?** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.
- Use the **pktcnt** keyword to specify the maximum number of packets to be traced. IP packet tracing will automatically be disabled when the specified number of packets is traced, or the trace buffer fills up. If a packet count is not specified, a circular trace buffer is used. The default trace buffer size is 131072 bytes.
 - Use the **pktsize** keyword to specify the maximum number of bytes to trace per packet. This value must be in the range of 14 to 1024. The default number of bytes to trace per packet is 128.
 - Use the **show debug interface** command to display statistics about the packet trace and to display the contents of the trace buffer in hex.



Note

IP packet tracing must be disabled on the interface before the trace buffer can be displayed.

Examples

The following example enables IP packet tracing on the *ge2* interface:

```
[SN5428-2A]# debug interface ge2 trace enable
```

The following example enables IP packet tracing on *ge1*, for a maximum of 100 packets. A maximum of 200 bytes will be traced per packet.

```
[SN5428-2A]# debug interface ge1 trace pktsent 100 pktsize 200 enable
```

Related Commands

Command	Description
show debug	Display a variety of debug information or perform specific troubleshooting activities.
show debug interface ge?	Display IP packet trace statistics or the contents of the trace buffer.

debug ip rip

To enable routing information protocol (RIP) debug log message, use the **debug ip rip** command. To disable RIP debug log message, use the **no** form of this command.

debug ip rip
no debug ip rip

Syntax Description	This command has no arguments or keywords.				
Defaults	RIP debug log messages are disabled.				
Command Modes	Administrator.				
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>3.2.1</td><td>This command was introduced.</td></tr></table>	Release	Modification	3.2.1	This command was introduced.
Release	Modification				
3.2.1	This command was introduced.				
Usage Guidelines	The debug ip rip command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.				

Examples

The following example enables RIP, configures logging to send debug message to all virtual terminal sessions, and then enables RIP debug log messages. The **show ip rip** command is used to verify the running RIP configuration.

```
[SN5428-2A]# ip rip enable
Dec 09 16:12:50: %IP-5-IRMRSAR: RIP Services are running
*[SN5428-2A]# logging level debug from ip to vty
*[SN5428-2A]# debug ip rip
Dec 31 12:52:14: %IP-7-IRRPRL00: RIP Packet received from 10.1.30.1 length 124
Dec 31 12:52:14: %IP-7-IRRPRL01:   command 2 version 1
Dec 31 12:52:14: %IP-7-IRRPRL02:   route af 2, dest 10.1.40.0 mask 0.0.0.0 nextHop
0.0.0.0 metric 2
Dec 31 12:52:14: %IP-7-IRRPRL02:   route af 2, dest 10.1.51.0 mask 0.0.0.0 nextHop
0.0.0.0 metric 1

*[SN5428-2A]# show ip rip
Routing Information Protocol (RIP) Information:
  Invalid Timer: 180
  Enabled Flag:  true
  Debug Flag:   true
  Running Flag:  true
```


Related Commands	Command	Description
	ip rip enable	Enable the storage router to learn dynamic routing using the routing information protocol (RIP).
	show ip	Display entries from the SN 5428-2 Storage Router routing table, and statistics about the protocols used in the storage router network. Use the rip keyword to display RIP configuration information.

debug scsirouter

To enable trace facilities for debugging SCSI routing instances, use the **debug scsirouter** command. To disable debugging, use the **no** form of this command.

debug scsirouter *name* **scsitrace**

no debug scsirouter *name* **scsitrace**

Syntax Description

<i>name</i>	The name of the SCSI routing instance to be debugged.
scsitrace	Keyword indicating tracing services will be enabled.

Defaults

All trace facilities are enabled by default.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

When enabled at this level, debug tracing will trace traffic to and from all targets associated with the named SCSI routing instance. Use the **show debug scsirouter** command to view the trace buffer output.

Examples

The following example enables debug tracing facilities for a SCSI routing instance named *foo*:

```
[SN5428-2A] # debug scsirouter foo scsitrace
```

Related Commands

Command	Description
debug aaa	Enable debugging for AAA authentication services.
debug scsirouter iscsitrace	Enable iSCSI trace facilities for debugging connections to and from the specified SCSI routing instance.
debug scsirouter target	Enable debugging for a specific SCSI routing instance target and LUN combination.
show debug scsirouter	Display trace buffer output.

debug scsirouter iscsitrace

To enable trace facilities for debugging iSCSI connections to and from SCSI routing instances, use the **debug scsirouter iscsitrace** command. To disable iSCSI trace facilities, use the **no** form of this command.

```
debug scsirouter name iscsitrace [fromto {A.B.C.D/bits | A.B.C.D/1.2.3.4}] [pducnt nn]  
[pdu size nn] enable
```

```
no debug scsirouter name iscsitrace enable
```

Syntax Description

<i>name</i>	The name of the SCSI routing instance to be debugged.
fromto <i>A.B.C.D/bits</i>	(Optional) Trace iSCSI Protocol Data Units (PDUs) from and to the specified host or network. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style.
fromto <i>A.B.C.D/1.2.3.4</i>	(Optional) Trace iSCSI PDUs from and to the specified host or network. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask.
pducnt <i>nn</i>	(Optional) Specify the maximum number of PDUs to trace.
pdu size <i>nn</i>	(Optional) Specify the maximum trace size per PDU, in bytes.
enable	Enable iSCSI trace facilities.

Defaults

The following are the default iSCSI trace options:

- All client connections to and from the specified SCSI routing instance are traced.
- The maximum trace size per PDU is 48 bytes.
- All PDUs are traced (circular).
- The trace buffer size is 131072 bytes. This value cannot be changed.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced.

Usage Guidelines

The **debug scsirouter iscsitrace** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

Use the **show debug scsirouter** command with the **iscsitrace** keyword to display iSCSI trace information.

Examples

The following example enables iSCSI trace facilities for the SCSI routing instance named *zeus*, using the default iSCSI trace options:

```
[SN5428-2A] # debug scsirouter zeus iscsitrace enable
```

Related Commands

Command	Description
debug scsirouter	Enable debugging for the named SCSI routing instance.
debug scsirouter target	Enable debugging for a specific SCSI routing instance target and LUN combination.
show debug scsirouter	Display trace buffer output.

debug scsirouter target

To enable trace facilities for debugging a specific SCSI routing instance target and LUN combination, use the **debug scsirouter target** command. To disable debugging, use the **no debug scsirouter target** form of this command.

debug scsirouter *name* **target** *name* **lun** *nn* **scsitrace**

no debug scsirouter *name* **target** *name* **lun** *nn* **scsitrace**

Syntax Description

<i>name</i>	The name of the SCSI routing instance to be debugged.
target <i>name</i>	The name of the target to be included in the trace.
lun <i>nn</i>	The specific LUN associated with the target.
scsitrace	Keyword indicating tracing services will be enabled.

Defaults

All trace facilities are enabled by default.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

When enabled at this level, SCSI tracing will trace traffic to and from the specified target and LUN combination associated with the named SCSI routing instance. Use the **show debug scsirouter** command to view the trace buffer output.

Examples

The following example enables SCSI tracing facilities for the target and LUN combination *myTarget*, LUN 0, associated with the SCSI routing instance named *foo*:

```
[SN5428-2A] # debug scsirouter foo target myTarget lun 0 scsitrace
```

Related Commands

Command	Description
debug aaa	Enable debugging for AAA authentication services.
debug scsirouter	Enable debugging for the named SCSI routing instance.
debug scsirouter iscsitrace	Enable iSCSI trace facilities for debugging connections to and from the specified SCSI routing instance.
show debug scsirouter	Display trace buffer output.

delete accesslist

To delete an entire access list, all access lists, or a specified entry from the named access list, use the **delete accesslist** command. This command does not change the persistent storage router configuration until the relevant configuration information has been saved using the appropriate **save** command with the **bootconfig** keyword.

```
delete accesslist all

delete accesslist name [A.B.C.D/bits | A.B.C.D/1.2.3.4]

delete accesslist name [chap-username username | iscsi-name string]

delete accesslist name all
```

Syntax Description		
	<i>name</i>	The name of the access list.
	<i>A.B.C.D/bits</i>	(Optional) IP address and subnet mask of the IP host being deleted from the access list. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style.
	<i>A.B.C.D/1.2.3.4</i>	(Optional) IP address and subnet mask of the IP host being deleted from the access list. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask.
	chap-username <i>username</i>	(Optional) The CHAP user name configured for the IP host being deleted from the access list. The CHAP user name is used for iSCSI authentication purposes.
	iscsi-name <i>string</i>	(Optional) The iSCSI Name of the IP host being deleted from the access list.
	<i>name</i> all	Delete all entries from the named access list.
	all	Delete all access lists.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Because access lists are cluster entities, this operation affects all targets associated with this access list, regardless of where the associated SCSI routing instance is running within the high availability cluster.

- Use the **delete accesslist name all** to clear all entries from the access list, but retain the access list entity.
- Use the **delete accesslist name** command with no additional parameters to completely delete the named access list. Before completely deleting an access list, verify that it is no longer associated with any SCSI routing instance target.

Changes to access lists do not impact currently connected IP hosts; changes are effective for all subsequent connections.

**Note**

If you delete an access list that is still associated with a SCSI routing instance target, the target remains bound to the access list, but subsequent connection requests by IP hosts will be rejected (as if the **scsirouter target accesslist none** command had been issued). Use the **show scsirouter** command with the **target** keyword to view access lists associated with SCSI routing instance targets.

In a cluster environment, access list management functions are handled by a single storage router. To determine which storage router is performing access list management functions, issue the **show cluster** command. If you issue a **delete accesslist** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information on operating the storage router in a cluster.

Examples

The following example completely deletes the access list named *fooList* from the currently running configuration:

```
[SN5428-2A] # delete accesslist fooList
```

The following example deletes all entries from the access list named *fooList1*. The access list entity itself is not deleted from the currently running configuration:

```
[SN5428-2A] # delete accesslist fooList1 all
```

The following example deletes all access lists from the currently running configuration:

```
[SN5428-2A] # delete accesslist all
```

The following example deletes the specified IP address from the named access list, *fooList2*. This command does not update the bootable configuration of the storage router until a **save accesslist bootconfig** or **save all bootconfig** command is issued.

```
[SN5428-2A] # delete fooList2 192.168.54.12/32
```

The following example deletes the specified CHAP user name from the named accesslist, *fooList3*. This command does not update the bootable configuration of the storage router until a **save accesslist bootconfig** or **save all bootconfig** command is issued.

```
[SN5428-2A] # delete fooList3 chap-username webserver15
```


The following example deletes the specified iSCSI Name from the named accesslist, *fooList4*. This command does not update the bootable configuration of the storage router until a **save accesslist bootconfig** or **save all bootconfig** command is issued.

```
[SN5428-2A]# delete fooList4 iscsi-name ign.1987-05.com.cisco.01.8838a325b4017f
```

Related Commands	Command	Description
	accesslist	Create an access list entity.
	accesslist A.B.C.D/bits	Add IP addresses to an access list.
	accesslist chap-username	Add CHAP user name entries to an access list.
	accesslist iscsi-name	Add iSCSI Name entries to an access list.
	restore accesslist	Restore the named access list or all access lists from the named configuration file.
	save accesslist	Save configuration data for the named access list or for all access lists.
	scsirouter target accesslist	Associate an access list with a specific SCSI routing target or all targets.
	show accesslist	Display the contents of the named access list or all access lists.

delete fcalias

To delete the named alias, or the specified member WWPN from the named alias, use the **delete fcalias** command.

delete fcalias *alias-name* [**member wwpn** *xxxxxxxxxxxxxxxx*]

Syntax Description

<i>alias-name</i>	The name of the alias.
member wwpn <i>xxxxxxxxxxxxxxxx</i>	The WWPN of the alias member.
Note	WWPN address notation is represented by 16 hex digits. The digits may be separated by colons. When entering WWPN addresses, colons can be omitted or placed anywhere in the address notation as long as they do not leave one character without a partner character.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

An alias is a collection of Fibre Channel devices, such as switches, initiators, storage and other SN 5428-2 Storage Routers, that can be zoned together. An alias is not a zone and cannot include a zone or another alias as a member.

Use this command to delete an entire alias and all its members from the zoning database, or to delete a specified member WWPN from an alias.

If the alias is a member of the active zone set, the alias will not be removed from the active zone set until the active zone set is deactivated. Use the **no zoneset** command with the **enable** keyword to deactivate the active zone set.



Caution

If the storage router is connected to the FC switched fabric, all zoning changes (including the deletion of an alias) are immediately propagated to other SN 5428-2 Storage Routers and switches in the fabric.

See [Chapter 5, “Configuring Fibre Channel Interfaces,”](#) for more information about FC fabric zoning.

Examples

The following example deletes the alias named *AliasFoo* and all its members. The alias will be removed from all zone sets in which it is used.

```
[SN5428-2A] # delete fcalias AliasFoo
```


The following example deletes the member WWPN *21000004ed4105ab* from the alias *AliasFoo*:

```
[SN5428-2A]# delete fcalias AliasFoo member wwpn 21000004ed4105ab
```

Related Commands

Command	Description
fcalias	Create an alias entity for use in Fibre Channel zoning.
fcalias member	Add the specified member to the named alias.
show fcalias	Display information about aliases and their members.

delete fcip

To delete the named elements from the FCIP instance, or to delete the named instance or all FCIP instances, use the **delete fcip** command. This command does not change the persistent storage router configuration until the relevant configuration information has been saved using the appropriate **save** command with the **bootconfig** keyword.

delete fcip {*name* | **all**}

delete fcip *name* **destination** *name*

Syntax Description

<i>name</i>	The name of the FCIP instance.
all	Keyword, used to delete all FCIP instances from the storage router.
	Note You are not prompted to confirm your actions.
destination <i>name</i>	The name of the specific destination to delete.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced.

Usage Guidelines

Use this command if you want to reconfigure the FCIP instance. You can delete the peer destination or the entire FCIP instance, or all FCIP instances. You must save the configuration changes to update the storage router bootable configuration.

Examples

The following examples deletes a destination named *dest2* from the FCIP instance, *fcip2*:


```
[SN5428-2A] # delete fcip fcip2 destination dest2
```

The following example deletes all FCIP instances:

```
[SN5428-2A] # delete fcip all
```

The following example deletes the FCIP instance named *fcip1*:

```
[SN5428-2A] # delete fcip fcip1
```


 delete fcip

Related Commands	Command	Description
	fcip	Create an FCIP instance.
	show fcip	Display configuration and operational information for the named FCIP instance.

delete logging

To delete a rule from the logging table, use the **delete logging** command.

delete logging level *notification-level* **from** *facility-name*

delete logging **#?**

delete logging **#nn**

Syntax Description

level <i>notification-level</i>	The notification level of the routing rules entry to be deleted. See Table 12-4 in the Usage Guidelines section for a list of valid names that can be used for the <i>notification-level</i> argument.
from <i>facility-name</i>	The name of the facility. A facility is the feature area from which the message is received. See Table 12-5 in the Usage Guidelines section for a list of valid facility names.
#?	Request an indexed list of entries in the logging table.
#nn	The index number from the displayed list of entries. The specified routing rule will be deleted.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Event, trace and debug messages can be routed to various destinations, based on the notification level of the message and the application area (facility) that generated the message. When a log message is received by the storage router, the logging table rules are searched by facility name and by message level until a match is found. The log message is sent to all the destinations specified by the matching rule.

Use this command to delete logging rules based on notification level and facility name, or by index number.

To display an indexed lists of entries in the logging table, use the number sign (#) character followed by a question mark (?). That action will cause the routing rules in the logging table to be displayed as a numbered (indexed) set of lines. The command is displayed at the prompt below the list to the point of the # keyword. Complete the command by entering the appropriate index number. The specified routing rule will be deleted.

The level limits logging to messages of the specified level or lower levels, based on level number. [Table 12-4](#) describes the available logging levels.

Table 12-4 Logging Level Notification Levels and Corresponding Numbers

Notification Level	Level Number	Description
emergency	0	System unusable
alert	1	Immediate action needed
critical	2	Critical conditions
error	3	Error conditions
warning	4	Non-fatal warning conditions
notice	5	Normal but significant conditions
info	6	Informational messages only
debug	7	Information for troubleshooting purposes

**Note**

The debug notification level should be used for specific troubleshooting purposes only. System performance and HA behavior may be adversely affected by logging at the debug notification level.

Each facility can have up to eight notification levels. Each facility and notification level pair can have up to seven destinations. [Table 12-5](#) describes the available facility names.

Table 12-5 Logging Level Facilities

Facility Name	Description
all	All facilities.
AUTH	AAA authentication.
CDP	Cisco Discovery Protocol.
CONF	Configuration functions.
FC	Fibre Channel interfaces.
FCIP	FCIP functions.
GE	Gigabit Ethernet interfaces.
HA	High availability cluster functions.
IF	Interface manager.
INVALID	Generic functions.
IP	IP functions.
ISCSI	iSCSI functions.
MON	Hardware monitor.
SLP	Service Location Protocol service functions.
SNMP	Simple Network Management Protocol.
SYSLOG	Syslog functions.
UI	User interface functions.
VTP	VTP and VLAN functions.

Use the **save system bootconfig** or **save all bootconfig** commands to save the updated logging table.

Examples

The following example displays the logging table and then deletes the routing rule entry for messages at level *info* from facility *all*:

```
[SN5428-2A]# show logging
Logging is enabled

Index Level      Priority Facility  Route
1      info       6          all      console logfile
2      debug      7          HA       logfile rslog

Syslog host is enabled, ip-address is 10.1.1.144

[SN5428-2A]# delete logging level info from all
```

The following example displays an indexed list of the routing rules in the logging table and then deletes the third entry:

```
[SN5428-2A]# delete logging #?

Logging is enabled

Index Level      Priority Facility  Route
1      critical    2          all      console logfile
2      debug       7          SNMP     rslog
3      notice      5          HA       all
4      warning     4          CDP      rslog

Syslog host is enabled, ip-address is 10.1.1.144

[SN5428-2A]# delete logging #3
```

Related Commands

Command	Description
clear logging table	Clear the SN 5428-2 Storage Router logging table of all entries, or to reset the table to factory defaults.
logging #?	Insert a routing rule entry into the storage router logging table.
logging level	Add rule entries to route storage router event, debug and trace messages to various destinations based on facility and notification level.
logging on	Enable or temporarily disable logging of storage router event message.
show logging	Display the routing rules in the logging table and the contents of the storage router log file.

delete savedconfig

To remove the named file from the *savedconfig* directory, use the **delete savedconfig** command.

delete savedconfig {*filename* | **all**}

Syntax Description	<i>filename</i>	The name of the configuration file to be deleted. This file must exist in the <i>savedconfig</i> directory.
	all	Keyword, indicating that all configuration files in the <i>savedconfig</i> directory are to be deleted.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use the **show savedconfig** command to display the contents of the *savedconfig* directory.

Examples The following example removes the configuration file named *foo_config* from the storage router:

```
[SN5428-2A] # delete savedconfig foo_config
```

Related Commands	Command	Description
	copy	Copy the named configuration or script file from a remote location to the storage router, or from the storage router to a remote location.
	restore all	Restore the contents of the named configuration file into memory.
	save all	Save all configuration information.
	save system	Save selected system configuration information
	show savedconfig	Display the contents of the <i>savedconfig</i> directory or the contents of the named configuration file.
	show script	Display the contents of the script directory or the contents of the named command file.

delete script

To remove the named command file from the *script* directory, use the **delete script** command.

delete script {*filename* | **all**}

Syntax Description	<i>filename</i>	The name of the command file to be deleted. This file must exist in the <i>script</i> directory.
	all	Keyword, indicating that all command files in the <i>script</i> directory are to be deleted.

Defaults	None.
-----------------	-------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use the show script command to display the contents of the <i>script</i> directory or the specified command file.
-------------------------	--

Examples	The following example removes the command file named <i>foo_script</i> from the storage router:
-----------------	---

```
[SN5428-2A] # delete script foo_script
```


Related Commands	Command	Description
	copy	Copy the named configuration or script file from a remote location to the storage router, or from the storage router to a remote location.
	read script	Read and execute the CLI commands in the named script file.
	restore all	Restore the contents of the named configuration file into memory.
	save all	Save all configuration information.
	save system	Save selected system configuration information.
	show bootconfig	Display the bootable configuration, or create a command file based on the bootable configuration.
	show runningconfig	Display the running configuration, or create a command file based on the running configuration.
	show savedconfig	List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file.
	show script	Display the contents of the script directory or the contents of the named command file.

delete scsirouter

To delete the named elements from the SCSI routing instance, use the **delete scsirouter** command. This command does not change the persistent storage router configuration until the relevant configuration information has been saved using the appropriate **save** command with the **bootconfig** keyword.

delete scsirouter {*name* | **all**} [**connection** *nn* | **serverif** *ge?* [**vlan** *vid*]]

delete scsirouter {*name* | **all**} **serverif** *ge?* **force**

delete scsirouter {*name* | **all**} **target** {*name* | **all**} [**lun** *nn*]

delete scsirouter {*name* | **all**} **target** {*name* | **all**} [**lun** *nn*] **force**

delete scsirouter {*name* | **all**} **force**

delete scsirouter *name* **all**

Syntax Description		
<i>name</i>		The name of the SCSI routing instance.
all		Delete all SCSI routing instances from the storage router, or delete all attributes for the named SCSI routing instance.
		Note You are not prompted to confirm your actions.
connection <i>nn</i>		(Optional) Delete the specified connection from the named instance or all instances. Use the show scsirouter command with the connection keyword to display connection IDs.
serverif <i>ge?</i>		(Optional) Delete the server interface for the named SCSI routing instance or all instances.
vlan <i>vid</i>		(Optional) Delete the specified VLAN from the named SCSI routing instance or all instances.
target <i>name</i>		The name of the specific target to delete.
target all		Delete all targets from the named instance.
lun <i>nn</i>		(Optional) Delete the specified iSCSI LUN from the named target or all targets.
force		(Optional) Keyword that overrides normal protections, allowing the action to be performed.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

In a cluster environment, changes to the SCSI routing instance can only be made on the storage router that is the currently running that instance. The SCSI routing instance may be in a stopped state at the time it is deleted.

The **force** option allows the SCSI routing instance to be deleted from a storage router that is not currently running the instance. The **force** option should only be used when the storage router, or a specific SCSI routing instance, is in an abnormal state and cannot be recovered without rebooting.

When used with the target or LUN keywords, the **force** option allows the specified object to be deleted, even if in use by an iSCSI driver. Under normal circumstances, a target or LUN cannot be deleted if an iSCSI driver is logged in.

Use the **all** keyword to delete all attributes of a named SCSI routing instance. The named SCSI routing instance, however, is not deleted.

**Note**

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

Examples

The following example deletes all targets associated with the SCSI routing instance named *foo*:

```
[SN5428-2A] # delete scsirouter foo target all
```

The following example deletes the specified VLAN from the Gigabit Ethernet interface, *ge2*, used by the SCSI routing instance named *foo2*:

```
[SN5428-2A] # delete scsirouter foo2 serverif ge2 vlan 101
```

The following example deletes all attributes of the SCSI routing instance named *foo3*. The SCSI routing instance named *foo3* remains available for configuration on the storage router.

```
[SN5428-2A] # delete scsirouter foo3 all
```

The following example deletes the entire SCSI routing instance named *foo4*:

```
[SN5428-2A] # delete scsirouter foo4
```

**Note**

All examples update the currently running configuration only. To make a deletion permanent, issue the appropriate **save all bootconfig** or **save scsirouter bootconfig** command.

Related Commands	Command	Description
	restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	scsirouter	Create a SCSI routing instance.
	scsirouter enable	Start and stop the named SCSI routing instance.
	scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
	scsirouter target maxcmdqueuedepth	Specify the maximum number of commands allowed at any given time from each iSCSI session to the specified target.
	setup scsi	Run the wizard to configure a SCSI routing instance.
	show accesslist	Display the contents of the named access list or all access lists.
	show scsirouter	Display configuration and operational information for the named SCSI routing instance.

delete software version

To delete a version of software from the storage router, use the **delete software version** command.



Note

The version of software currently running and the version that will be booted when the system is restarted may not be deleted.

delete software version {v.x.y | all}

Syntax Description

v.x.y	The version of storage router software to be deleted.
all	Delete all non-bootable and non-current software versions.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to remove old versions of software from the storage router.

Examples

The following example removes version 2.0.1 from the storage router:

```
[SN5428-2A] # delete software version 2.0.1
```

Related Commands

Command	Description
download software	Download the list of available software versions or the specified version of software from the named location.
software http url	Specify the default location from which to download updated storage router software via HTTP.
software proxy url	Specify the default location from which to download updated storage router software via HTTP, using a proxy server.
software tftp	Specify the default location from which to download updated storage router software via TFTP.
verify software version	Check the specified software version for problems.

delete zone

To delete the specified Fibre Channel (FC) zone or the specified member of the zone from the zoning database, use the **delete zone** command.

delete zone *name* [**member** {**fcalias** *alias-name* | **fcid** *port-id* | **wwpn** *xxxxxxxxxxxxxxxx*}]

Syntax Description

<i>name</i>	The name of the zone.
member	(Optional) Keyword, indicating the specified zone member will be deleted.
fcalias <i>alias-name</i>	Deletes the named alias member from the named zone.
fcid <i>port-id</i>	Deletes the specified Port ID member from the named zone.
wwpn <i>xxxxxxxxxxxxxxxx</i>	Deletes the specified WWPN member from the named zone.
	Note WWPN address notation is represented by 16 hex digits. The digits may be separated by colons. When entering WWPN addresses, colons can be omitted or placed anywhere in the address notation as long as they do not leave one character without a partner character.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

A zone is a group of FC ports or devices, such as switches, storage or SN 5428-2 Storage Routers, grouped together to control the exchange of information.

Use this command to delete the specified zone from the zoning database. If the zone is a member of the active zone set, the zone will not be removed from the active zone set until the active zone set is deactivated. Use the **no zoneset** command with the **enable** keyword to disable the active zone set.

Use the **member** keyword to delete the specified alias, Port ID or WWPN member from the named zone.



Caution

If the storage router is connected to the FC switched fabric, all zoning changes (including the deletion of a zone or zone member) are immediately propagated to other SN 5428-2 Storage Routers and switches in the fabric.

See [Chapter 5, “Configuring Fibre Channel Interfaces,”](#) for more information about FC fabric zoning.

Examples

The following example deletes the zone named *testlab* from the zoning database:

```
[SN5428-2A]# delete zone testlab
```

The following example deletes the alias member *myfoo* from the zone *webservices*:

```
[SN5428-2A]# delete zone webservices member fcalias myfoo
```

Related Commands

Command	Description
show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
zone	Create a Fibre Channel fabric zone.
zone member	Add a device or an alias to a zone.
zoneset	Create a Fibre Channel fabric zone set.
zoneset zone	Add a member zone to a zone set.

delete zoneset

To delete the specified zone from the zone set or to delete the entire named zone set from the zoning database, use the **delete zoneset** command.

delete zoneset *name* [*zone name*]

Syntax Description

<i>name</i>	The name of the zone set.
<i>zone name</i>	(Optional) Deletes the named zone from the specified zone set.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

A zone set is a group of zones. Zoning enables you to divide the ports and devices of the Fibre Channel fabric into zones for more efficient and secure communication among functionally grouped nodes. Only one zone set can be active at a time. The active zone set defines the zoning for the Fibre Channel fabric.

Use this command to delete an entire zone set from the zoning database or only the named zone from the zone set. If the zone set is active, the command does not take effect until the zone set is deactivated. Use the **no zoneset** command with the **enable** keyword to disable the active zone set.



Caution

If the storage router is connected to the FC switched fabric, all zoning changes (including the deletion of a zone set) are immediately propagated to other SN 5428-2 Storage Routers and switches in the fabric.

See [Chapter 5, “Configuring Fibre Channel Interfaces,”](#) for more information about FC fabric zoning.

Examples

The following example deletes the zone set named *testgroup*:

```
[SN5428-2A] # delete zoneset testgroup
```

The following example deletes the zone named *zoneA* from the zoneset named *testgroupA*:

```
[SN5428-2A] # delete zoneset testgroupA zone zoneA
```


Related Commands	Command	Description
	show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
	show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
	zone	Create a Fibre Channel fabric zone.
	zone member	Add a device or an alias to a zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset zone	Add a member zone to a zone set.

download software

To fetch the specified object from the named location or the default download location, use the **download software list** command.

```
download software {http | proxy} {list | url full_url | version v.x.y}
```

```
download software tftp {hostname host filename file | list | version v.x.y}
```

Syntax Description		
http		Download using the HTTP protocol.
proxy		Download using a proxy server.
list		(Optional) Download a list of available versions.
url		(Optional) Keyword indicating that the download is from the specified URL.
<i>full_url</i>		The fully qualified URL from which to download this version of storage router software. For example, <code>http://anywebserver.com/3.3.1-K9.tar</code> .
version <i>v.x.y</i>		(Optional) Download the specified version of storage router software from the default location.
tftp		Download using the TFTP protocol
hostname <i>host</i>		The name of the TFTP host.
filename <i>file</i>		The name of the file to be downloaded, such as <code>3.3.1-K9.tar</code> . This file contains the storage router software.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines The list of available software versions is stored in the file named `sw-sn5428-2-versions.txt`. This text file must contain one line for each version of software that is available from the download location. If you store and download software from a site other than the system default (`http://www.cisco.com`), create this file and update it whenever a new version of software is available.

Software is either downloaded from the default locations set for the specified protocol or from the location specified as part of the command. Always verify software after it has downloaded to assure no errors were encountered. See [“Installing Updated Software”](#) for details on verification and making updated software available to the storage router.

A maximum of two versions of software can be stored on the SN 5428-2 Storage Router.

**Note**

While the size of the software file may vary, it will exceed 16 MB. Some older TFTP implementations have a 16 MB download limitation.

Examples

The following example downloads storage router software version 3.3.1-K9 from the default location via standard Hypertext Transfer Protocol (HTTP):

```
[SN5428-2A]# download software http version 3.3.1-K9
```

The following example downloads a file named *sn5428-2v331.tar* from the TFTP host named *my_tftpHost*. The file must exist in the default TFTP directory.

```
[SN5428-2A]# download software tftp hostname my_tftpHost filename sn5428-2v331.tar
```

The following file downloads the list of available software from the default location using the proxy configuration:

```
[SN5428-2A]# download software proxy list
```

Related Commands

Command	Description
delete software version	Remove the specified version of software from the storage router.
software http url	Specify the default location from which to download updated storage router software via HTTP.
software http username	Configure the user name and optional password required to access the default download location.
software proxy	Configure HTTP proxy information.
software proxy url	Specify the default location from which to download updated storage router software via HTTP, using a proxy server.
software proxy username	Configure the user name and optional password required to access the proxy URL.
software tftp	Specify the default location from which to download updated storage router software via TFTP.
verify software version	Check the specified software version for problems.

enable

To change the management session from Monitor mode to Administrator mode, use the **enable** command. Monitor mode, which is the default mode, provides view-only access to the storage router management interface. Administrator mode allows you to create entities and make changes to the configuration of the storage router.

enable

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Monitor.
----------------------	----------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Issue the enable command after a successful CLI login to change to Administrator mode. You are prompted to enter the Administrator mode password, if required. Use the exit command to return to Monitor mode.
-------------------------	--

Examples	The following example changes the session from Monitor mode to Administrator mode.
-----------------	--

```
[SN5428-2A]# enable
```

```
Enter admin password: *****
[Entering Administrator mode]
```

Related Commands	Command	Description
	aaa authentication	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
	enable	
	exit	Leave Administrator mode and enter Monitor mode.
	logout	Terminate the management session.
	show aaa	Display AAA configuration information.

exit

To return the management session to Monitor mode from Administrator mode, use the **exit** command.

exit

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Issue the exit command to return to Monitor mode after previously issuing the enable command.
-------------------------	---

Examples	The following example returns the CLI session to Monitor mode: <pre>[SN5428-2A] # exit [Leaving Administrator mode]</pre>
-----------------	---

Related Commands	Command	Description
	enable	Enter Administrator mode.
	logout	Terminate the management session.

failover eligibility

To enable failover by eligibility for all SCSI routing instances running on the storage router, use the **failover eligibility** command. To disable failover by eligibility, use the **no** form of this command.

failover eligibility on

no failover eligibility on

Syntax Description	on	Keyword used to enable failover by eligibility for all SCSI routing instances running on the storage router.
--------------------	----	--

Defaults	Failover by eligibility is enabled.
----------	-------------------------------------

Command Modes	Administrator mode.
---------------	---------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Each storage router in a cluster maintains and exchanges information about available resources. Failover by eligibility is enabled by default; HA bases the decision to automatically fail over a SCSI routing instance to another node in a cluster based on the Fibre Channel and other resources available to that SCSI routing instance.
------------------	--

Failover occurs when:

- All mapped targets are unavailable or a critical resource for the SCSI routing instance is unavailable, and some or all mapped targets would be available from another node in the cluster. A critical resource can be a configured Gigabit Ethernet interface, a required Fibre Channel interface, or an internal resource needed to run the SCSI routing instance.
- Some mapped targets are unavailable and all mapped targets are available on another node in the cluster.
- All mapped targets are available, but another node in the cluster also has all targets available and is designated as the primary for the SCSI routing instance.
- The storage router stops receiving heartbeats from another node within the cluster.

For more manual control over where a SCSI routing instance runs, use the **no failover eligibility on** command to prevent failover by eligibility on a storage router. If a SCSI routing instance is running on (or fails over to) a storage router that is configured with failover by eligibility turned off, it will continue running on that storage router unless there are no mapped targets available or a critical resource is unavailable.

Use the **failover eligibility on** command to restore normal failover functions.

The failover eligibility setting is not retained across a reboot; restarting the storage router restores the default setting (failover by eligibility is enabled).

Examples

The following example disables failover by eligibility for all SCSI routing instances running on the storage router named SN 5428-2A:

```
[SN5428-2A] no failover eligibility on
```

Related Commands

Command	Description
failover scsirouter	Cause the named SCSI routing instance to cease running on the storage router.
show ha	Display HA operational statistics for the storage router or for a specific application.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

failover scsirouter

To cause the named SCSI routing instance to cease running on this storage router and start running on another storage router in the cluster, use the **failover scsirouter** command.

**Note**

If no eligible storage router is found, the SCSI routing instance will start running again on the same node. If the storage router is configured as a standalone system, failover is not allowed.

failover scsirouter *name* [**pri** | **sec** | **to systemname**]

failover scsirouter **all** [**to systemname**]

Syntax Description

<i>name</i>	The name of the SCSI routing instance to be failed over.
all	Failover all instances currently running on this storage router.
pri	(Optional) Force failover to the designated primary storage router on the failover list.
sec	(Optional) Force failover to the designated secondary storage router on the failover list.
to systemname	(Optional) Perform the failover to the specified storage router. This node must be active in the cluster.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use the **all** keyword to failover all SCSI routing instances currently running on this storage router. Each storage router can run a maximum of 12 SCSI routing instances; there is a maximum of 12 SCSI routing instances per cluster.

Examples

The following example causes the SCSI routing instance named *foo* to failover to another storage router in the cluster:

```
[SN5428-2A] # failover scsirouter foo
```

The following example causes all SCSI routing instances to failover to the storage router named *TestLab1*:

```
[SN5428-2A] # failover scsirouter all to TestLab1
```


Related Commands	Command	Description
	scsirouter enable	Stop or start the named SCSI routing instance.
	scsirouter failover	Add the storage router to the HA failover list for the specified SCSI routing instance.
	setup cluster	Change the configuration of the high availability environment.

fcalias

To create an alias entity for use in Fibre Channel zoning, use the **fcalias** command. An alias is a group of FC ports or devices (such as switches, storage or SN 5428-2 Storage Routers) that are grouped together for convenience.

fcalias *alias-name*

Syntax Description	<i>alias-name</i>	The name of the alias entity created by this command. Enter a maximum of 31 characters. The name must begin with an alpha character.
--------------------	-------------------	--

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines An alias allows you to group FC ports and devices together for zoning purposes. Unlike zones, however, aliases do not impose any communication restrictions on its members. An alias can belong to one or more zones, but a zone cannot be a member of an alias, nor can an alias be a member of another alias.

You must create a named alias entity before you can add members to the alias.

A default alias of *iscsi* is provided that contains both initiators WWPN1 and WWPN2.



Caution

If the storage router is connected to the FC switched fabric, all zoning changes (including the creation of an alias) are immediately propagated to other SN 5428-2 Storage Routers and switches in the fabric.

See [Chapter 5, “Configuring Fibre Channel Interfaces,”](#) for more information about FC fabric zoning.

Examples The following example creates an alias entity named *LabGroupA*:

```
[SN5428-2A] # fcalias LabGroupA
```

Related Commands	Command	Description
	delete fcalias	Delete the named alias or the specified alias member.
	fcalias member	Add the specified member to the named alias.
	show fcalias	Display information about aliases and their members.
	zone member	Add a device or an alias to a zone.

fcalias member

To add the specified member to the named alias, use the **fcalias member** command. An alias is a group of FC ports or devices (such as switches, storage or SN 5428-2 Storage Routers) that are grouped together for convenience.

fcalias *alias-name* **member wwpn** *xxxxxxxxxxxxxxxx*

Syntax Description	<i>alias-name</i>	The name of the alias entity.
	wwpn <i>xxxxxxxxxxxxxxxx</i>	The World Wide Port Name (WWPN) of the port or device to be added to the alias.
	Note	WWPN address notation is represented by 16 hex digits. The digits may be separated by colons. When entering WWPN addresses, colons can be omitted or placed anywhere in the address notation as long as they do not leave one character without a partner character.


Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines An alias allows you to group FC ports and devices together for zoning purposes. Unlike zones, however, aliases do not impose any communication restrictions on its members. An alias can belong to one or more zones, but a zone cannot be a member of an alias, nor can an alias be a member of another alias.

The command verifies the format of the WWPN, but does not verify that the specified device exists. A default alias of *iscsi* is provided that contains both initiators WWPN1 and WWPN2.



Caution

If the storage router is connected to the FC switched fabric, all zoning changes (including adding a member to an alias) are immediately propagated to other SN 5428-2 Storage Routers and switches in the fabric.

See [Chapter 5, “Configuring Fibre Channel Interfaces,”](#) for more information about FC fabric zoning.

Examples The following example creates the alias named *LabGroupA*, and then adds the devices with the WWPN *2200001026558a0f* and *220000201744ab3c* to the named alias:

```
[SN5428-2A] # fcalias LabGroupA
[SN5428-2A] # fcalias LabGroupA member wwpn 2200001026558a0f
[SN5428-2A] # fcalias LabGroupA member wwpn 220000201744ab3c
```


Related Commands	Command	Description
	delete fcalias	Delete the named alias or the specified alias member.
	fcalias	Create an alias entity for use in Fibre Channel zoning.
	show fcalias	Display information about aliases and their members.
	zone member	Add a device or an alias to a zone.

fcip

To create an FCIP instance, use the **fcip** command.

fcip *name*

Syntax Description	<i>name</i>	The name of the FCIP instance. Valid named are <i>fcip1</i> and <i>fcip2</i> .
Defaults	None.	
Command Modes	Administrator.	
Command History	Release	Modification
	3.3.1	This command was introduced.

Usage Guidelines

FCIP provides connectivity between SANs. Technically, it employs Fibre Channel over TCP/IP (FCIP) to provide block oriented FC devices connectivity over an IP network. FCIP allows the interconnection of islands of FC storage area networks (SANs) over IP-based networks to form a unified SAN in a single FC fabric. The FCIP instance becomes a binding point for the association of other configuration parameters.

An FCIP instance runs with a point-to-point connection to an FCIP instance on a peer SN 5428-2 Storage Router. Each FCIP instance requires one and only one peer.

There can be a maximum of 2 FCIP instances defined per storage router. Each FCIP instance is associated with:

- An internal FC interface *fc1* or *fc2* (*fc1* is initiator WWP1 and *fc2* is initiator WWP2). The FCIP instance named *fcip1* is associated with *fc1*; the instance named *fcip2* is associated with *fc2*. This association is made automatically.
- A network interface, which provides IP connectivity to the peer destination. The FCIP instance named *fcip1* uses the Gigabit Ethernet interface, *ge1*; the instance named *fcip2* uses *ge2*. If both Gigabit Ethernet interfaces are cabled to the same network, you can configure the FCIP instance to failover to the secondary interface in case of a failure on the primary interface.
- A destination, which is the IP address of the FCIP instance on the peer SN 5428-2 Storage Router. The destination configuration includes the connection protocol (TCP/IP or raw IP) used between the FCIP instances.

This command updates the running configuration of the storage router. You must save the FCIP instance configuration to the bootable configuration for it to be retained in the storage router when it is restarted. Issue the **save fcip** command with the **bootconfig** keyword to save the FCIP instance to the storage router bootable configuration.

Examples

The following example creates an FCIP instance named *fcip1*:

```
[SN5428-2A] # fcip fcip1
```

Related Commands

Command	Description
clear counters fcip	Reset accumulated operational statistics for the specified SCSI routing instance.
delete fcip	Delete the named FCIP instance or the specified element of the FCIP instance.
delete fcip	Enable debugging for the named FCIP instance.
fcip description	Add user-defined identification information to the named FCIP instance.
fcip destination config	Configure operational parameters for the named FCIP instance.
fcip destination raw	Add a peer destination to the named FCIP instance, with a connection type of raw IP.
fcip destination tcpclient	Add a peer destination to the named FCIP instance, with a connection type of TCP/IP. The named FCIP instance initiates the TCP connection.
fcip destination tcpserver	Add a peer destination to the named FCIP instance, with a connection type of TCP/IP. The named FCIP instance listens for the TCP connection from the named destination.
fcip enable	Stop or start the named FCIP instance.
fcip networkif	Assign a Gigabit Ethernet interface and IP address to the named FCIP instance.
restore fcip	Restore the named SCSI routing instance from the named configuration file.
save fcip	Save configuration information for the named FCIP instance.
show debug fcip	Display debugging information for the named FCIP instance.
show fcip	Display configuration and operational information for the named FCIP instance.

fcip description

To add user-defined identification information to the named FCIP instance, use the **fcip description** command.

fcip *name* **description** “*user text*”

Syntax Description

<i>name</i>	The name of this FCIP instance. Valid named are <i>fcip1</i> and <i>fcip2</i> .
“ <i>user text</i> ”	User-defined identification information associated with this FCIP instance. If the string contains spaces, enclose it in quotes. Enter a maximum of 64 characters.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced.

Usage Guidelines

This command allows you to add a new description or change an existing description. Descriptions are site-specific.

Examples

The following example adds the description “*Access to lab SAN island 7*” to the FCIP instance *fcip1*:

```
[SN5428-2A]# fcip fcip2 description “Access to lab SAN island 7”
```

Related Commands

Command	Description
fcip	Create an FCIP instance.
save fcip	Display configuration and operational information for the named FCIP instance.

fcip destination config

To configure operational parameters for the selected FCIP connection protocol type, use the **fcip destination config** command.

fcip *name* **destination** *name* **config** {*rxtcpwinsize* | *txtcpwinsize*} *nn*

fcip *name* **destination** *name* **config** *tcpport* *port-number*

fcip *name* **destination** *name* **config** {*bcouthiwater* | *burstouthiwater*} *nn*

fcip *name* **destination** *name* **config** *frouthiwater* *nn*

fcip *name* **destination** *name* **config** *peerneedsackhiwater* *nn*

fcip *name* **destination** *name* **config** {*initialtimeout* | *maxtimeout* | *totaltimeout*} *nn*

fcip *name* **destination** *name* **config** *ipprotocol* *nn*

fcip *name* **destination** *name* **config** *rexmitcount* *nn*

fcip *name* **destination** *name* **config** *timeoutincrement* *nn*

fcip *name* **destination** *name* **config** *frinhiwater* *nn*

fcip *name* **destination** *name* **config** *idlepingdelay* *nn*

fcip *name* **destination** *name* **config** *pktracemask* *mask*

fcip *name* **destination** *name* **config** *usebport* {*yes* | *no*}

Syntax Description

<i>name</i>	The name of this FCIP instance. Valid named are <i>fcip1</i> and <i>fcip2</i> .
destination <i>name</i>	The name of the peer destination.
rxtcpwinsize <i>nn</i>	The maximum number of outstanding bytes that can be received on a TCP connection. Valid values are 8192 to 2097152, inclusive. The default value is 262144. This configuration option applies to TCP client or TCP server connections only.
txtcpwinsize <i>nn</i>	The maximum number of outstanding bytes that can be transmitted on a TCP connection. Valid values are 8192 to 2097152, inclusive. The default value is 2097152. This configuration option applies to TCP client or TCP server connections only.
tcpport <i>port-number</i>	The TCP port number. The TCP server listens to this port; the TCP client connects to this port. Valid values are 0 to 65535, inclusive. The default port is 3225. This configuration option applies to TCP client or TCP server connections only.
bcouthiwater <i>nn</i>	The maximum number of bytes that can be outstanding on a raw IP connection. Valid values are from 1 to 4294967294, inclusive. The default value is 2097152. This configuration option applies to raw IP connections only.

burstouthiwater <i>nn</i>	The maximum number of bytes that can be transmitted on a raw IP connection. Valid values are from 1 to 4294967294, inclusive. The default value is 2097152. This configuration option applies to raw IP connections only.
frouthiwater <i>nn</i>	The maximum number of frames that can be outstanding on a raw IP connection. Valid values are from 1 to 4294967294, inclusive. The default value is 1024. This configuration option applies to raw IP connections only.
peerneedsackhiwater <i>nn</i>	The maximum number of unacknowledged frames that can exist at any given time on a raw IP connection. Valid values are from 0 to 4294967294. The default value is 16. This configuration option applies to raw IP connections only.
initialtimeout <i>nn</i>	The initial amount of time, in ticks, to delay before retransmitting a packet. This value is used in error recovery algorithms. Valid values are from 0 to 2147483647. The default value is 0. This configuration option applies to raw IP connections only.
maxtimeout <i>nn</i>	The maximum amount of time, in ticks, that can be used for any one retransmission, before the packet is discarded. This value is used in error recovery algorithms. Valid values are from 0 to 2147483647. The default value is 48 ticks. This configuration option applies to raw IP connections only. Note The default value is set to 48 ticks only if timeoutincrement , initialtimeout and totaltimeout keywords have no associated value.
totaltimeout <i>nn</i>	The maximum amount of time, in ticks, that a packet is kept alive, before it is discarded. This value is used in error recovery algorithms. Valid values are from 0 to 2147483647. The default value is 0. This configuration option applies to raw IP connections only.
ipprotocol <i>nn</i>	The value of the IP protocol used in the IP header. Valid values are from 0 to 255. The default value is 4. This configuration option applies to raw IP connections only. Note This should be a unique IP protocol value. Do not change this value to an IP protocol that is currently in use on the storage router. For example, do not change the value to the TCP protocol (6) or UDP protocol (17).
rexmitcount <i>nn</i>	The maximum number of times a packet can be retransmitted, before it is discarded. This value is used in error recovery algorithms. Valid values are from 1 to 2147483647. The default value is 4. This configuration option applies to raw IP connections only.
timeoutincrement <i>nn</i>	The amount of time, in ticks, to add to a packet's time out value before retransmitting the packet. This value increases the delay before the next retransmission, and is used in error recovery algorithms. Valid values are from 0 to 2147483647. The default value is 0. This configuration option applies to raw IP connections only.
frinhiwater <i>nn</i>	The maximum number of frames, received from a raw IP connection, that can be sent to the Fibre Channel (FC) interface. Valid values are from 1 to 4294967294. The default value is 688. This configuration option applies to all FCIP connection types.

idlepingdelay <i>nn</i>	The number of seconds before a keep-alive packet is sent across an idle connection. Valid values are 1 to 65535, inclusive. The default value is 60. This configuration option applies to all FCIP connection types.
pkttracemask <i>mask</i>	The value of the packet trace mask, in hex. Packets are traced for debugging problems. Valid values are 0 (0x0000) to 0xffff. A value of zero disables packet tracing. The default value is 0xffff, which enables all packet tracing. This configuration option applies to all FCIP connection types.
usebport yes	Use Fibre Channel (FC) B_Port connectivity. This configuration option applies to all FCIP connection types. This is the default.
usebport no	Do not use FC B_Port connectivity. This value should only be set if the SN 5428-2 is connected to another FCIP device that does not support B_Port connectivity.

Defaults

The following are the default settings for all FCIP connection configuration options:

- TCP receive window size—262144 bytes
- TCP transmit window size—2097152 bytes
- TCP port number—3225
- Maximum number of bytes outstanding on raw IP connection—2097152 bytes
- Maximum number of bytes transmitted on raw IP connection—2097152 bytes
- Maximum number of frames sent to FC interface—688 frames
- Maximum number of frames outstanding—1024 frames
- Maximum number of unacknowledged frames—16 frames
- Initial amount of delay before retransmission—0 ticks
- Maximum amount of time for retransmission—48 ticks
- Maximum amount of time a packet can be kept alive—0 ticks
- Value of IP protocol in IP header—4
- Maximum number of retransmissions—4
- The amount of time to increase the delay prior to retransmission—0 ticks
- The amount of time before a keep-alive ping is sent across an idle connection—60 seconds
- Packet trace mask—0xffff (packet tracing is enabled for all packets)
- The FCIP instance uses FC B_Port connectivity.

The default error recovery algorithm for raw connection protocol uses **maxtimeout** and **rexmitcount** values (timeout = **maxtimeout** / **rexmitcount**--).



Note

One second is approximately 60 ticks.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced.

Usage Guidelines

Each FCIP instance requires three active elements:

- The *networkif* element assigns an interface and IP address for use by the FCIP peer.
- The *destination* element assigns the peer's protocol and IP address.
- The device interface element associates the FCIP instance with an internal Fibre Channel interface and is automatically assigned and enabled.

An FCIP instance runs with a point-to-point connection to an FCIP instance on a peer SN 5428-2 Storage Router. Each FCIP instance requires one and only one peer. Both FCIP instances must be configured to use the same connection protocol, TCP/IP or raw IP.

TCP/IP connection protocol uses the FCIP standard and TCP flow control and error recovery algorithms. FCIP, using TCP connections, allows you to configure TCP receive and transmit window sizes. Raw IP uses a proprietary protocol, but allows you to configure a wider variety of operational settings, providing more granular control over flow control and error recovery. All changes to raw IP operational parameters are applied immediately. Changes to TCP operational parameters are not applied until the FCIP instance is stopped and restarted, or the storage router is rebooted.

Raw IP connections have unique flow control settings for network transmissions and FC transmissions. The FC transmission counter (the **frinhiwater** keyword) limits the number of frames given to the FC interface for transmission. The FC frames are only acknowledged once they have been transmitted out of the SN 5428-2. The network transmissions are controlled by both a byte counter (the **burstouthiwater** keyword) and a frame counter (the **frouthiwater** keyword). FCIP will not transmit data when either counter has reached its high water mark. The data is queued until the counters have receded from their high water mark.

Raw IP uses four error recovery algorithms. These algorithms use five different operational settings, which control which error recovery algorithm is used.

- **rexmitcount**—The maximum number of times a packet can be retransmitted, before it is discarded.
- **maxtimeout**—The maximum amount of time, in ticks, that can be used for any one retransmission, before the packet is discarded.
- **timeoutincrement**—The amount of time, in ticks, to add to a packet's time out value before retransmitting the packet.
- **initialtimeout**—The initial amount of time, in ticks, to delay before retransmitting a packet.
- **totaltimeout**—The maximum amount of time, in ticks, that a packet is kept alive, before it is discarded.

The following are the available error recovery algorithms:

1. For error recovery using **maxtimeout** and **rexmitcount**:

– timeout = **maxtimeout** / **rexmitcount**--

For example, using a **maxtimeout** value of 48 and **rexmitcount** value of 4 would result in retransmissions at 12, 16, 24 and 48 ticks. This is the default error recovery algorithm.

2. For error recovery using **timeoutincrement** and **rexmitcount**:

– timeout += **timeoutincrement**

For example, using a **timeoutincrement** value of 8 and a **rexmitcount** value of 4 would result in retransmissions at 8, 16, 24 and 32 ticks.

3. For error recovery using **timeoutincrement**, **initialtimeout** and **rexmitcount**:

- $\text{timeout} = \text{initialtimeout}$ /* initial calculation */
- $\text{timeout} = \text{timeout} * \text{timeoutincrement}$ /* subsequent calculations */

For example, using a **timeoutincrement** value of 2, an **initialtimeout** value of 8, and a **rexmitcount** of 4 would result in retransmissions at 8, 16, 32 and 64 ticks.

4. For error recovery using **totaltimeout** and **rexmitcount**:

- if (**rexmitcount** & 0x01) $\text{timeout} = ((\text{rexmitcount} - \text{remainingrexmitcount} + 1) * \text{totaltimeout}) / (\text{rexmitcount} * ((\text{rexmitcount} / 2) + (\text{rexmitcount} / 2)))$
- else $\text{timeout} = ((\text{rexmitcount} - \text{remaining rexmitcount} + 1) * \text{totaltimeout}) / (\text{rexmitcount} * ((\text{rexmitcount} * ((\text{rexmitcount} / 2) + (\text{rexmitcount} / 2)))$

For example, using a **totaltimeout** value of 48 and a **rexmitcount** value of 4 would result in retransmissions at 4, 9, 14 and 17 ticks.

By default, a raw IP connection uses the first error recovery algorithm. To use another error recovery algorithm, set the desired values for the appropriate operational settings. For example, to use the second error recovery algorithm, set the **timeoutincrement** and, optionally, the **rexmitcount**. To use the fourth error recovery algorithm, set the **totaltimeout** and, optionally, the **rexmitcount**.

Examples

The following example add the destination *dest1* to the FCIP instance named *fcip1*. The destination IP address is *10.1.40.27*. The FCIP instance is configured to use TCP/IP connection protocol and will initiate the connection (TCP client). The destinations TCP receive window size is set to 1 MB.

```
[SN5428-2A]# fcip fcip1 destination dest1 tcpclient 10.1.40.27
*[SN5428-2A]# fcip fcip1 destination dest1 config rxtcpwinsize 1048576
```

Related Commands

Command	Description
fcip	Create an FCIP instance.
fcip destination raw	Add a peer destination to the named FCIP instance, with a connection type of raw IP.
fcip destination tcpclient	Add a peer destination to the named FCIP instance, with a connection type of TCP/IP. The named FCIP instance initiates the TCP connection.
fcip destination tcpserver	Add a peer destination to the named FCIP instance, with a connection type of TCP/IP. The named FCIP instance listens for the TCP connection from the named destination.
fcip networkif	Assign a Gigabit Ethernet interface and IP address to the named FCIP instance.
show fcip	Display configuration and operational information for the named FCIP instance.

fcip destination raw

To add a peer destination to the named FCIP instance, with a connection type of raw IP, use the **fcip destination raw** command.

```
fcip name destination name raw A.B.C.D
```

Syntax Description

<i>name</i>	The name of the FCIP instance. Valid names are <i>fcip1</i> and <i>fcip2</i> .
destination <i>name</i>	The name of the peer destination. Enter a maximum of 31 characters.
<i>A.B.C.D</i>	The IP address of the peer destination. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The peer destination is the FCIP instance running in the partner SN 5428-2 Storage Router.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced.

Usage Guidelines

Each FCIP instance requires three active elements:

- The *networkif* element assigns an interface and IP address for use by the FCIP peer.
- The *destination* element assigns the peer’s protocol and IP address.
- The device interface element associates the FCIP instance with an internal Fibre Channel interface and is automatically assigned and enabled.

An FCIP instance runs with a point-to-point connection to an FCIP instance on a peer SN 5428-2 Storage Router. Each FCIP instance requires one and only one peer. Use this command to configure a peer destination name and IP address, using raw IP as the protocol type.

The destination IP address is the Gigabit Ethernet IP address of the FCIP instance running in the peer SN 5428-2 Storage Router. Both FCIP instances must be configured to use the same connection protocol.

Raw IP uses a proprietary connection protocol, but provides more operational control over flow control and error recovery than standard TCP/IP.



Note

When configuring an FCIP instance, you must configure the network interface before you configure the peer destination and protocol.

Examples

The following example configures the FCIP instance named *fcip1* with a destination named *lucky* at IP address *10.1.3.47*, using raw IP connection protocol:

```
[SN5428-2A]# fcip fcip1 destination lucky raw 10.1.3.47
```

Related Commands

Command	Description
fcip	Create an FCIP instance.
fcip destination config	Configure operational parameters for the named FCIP instance.
fcip networkif	Assign a Gigabit Ethernet interface and IP address to the named FCIP instance.
show fcip	Display configuration and operational information for the named FCIP instance.

fcip destination tcpclient

To add a peer destination to the named FCIP instance, with a connection type of TCP/IP, use the **fcip destination tcpclient** command. The named FCIP instance will initiate the TCP connection.

```
fcip name destination name tcpclient A.B.C.D
```

Syntax Description

<i>name</i>	The name of the FCIP instance. Valid names are <i>fcip1</i> and <i>fcip2</i> .
destination <i>name</i>	The name of the peer destination. Enter a maximum of 31 characters.
<i>A.B.C.D</i>	The IP address of the peer destination. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The peer destination is the FCIP instance running in the partner SN 5428-2 Storage Router.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced.

Usage Guidelines

Each FCIP instance requires three active elements:

- The *networkif* element assigns an interface and IP address for use by the FCIP peer.
- The *destination* element assigns the peer’s protocol and IP address.
- The device interface element associates the FCIP instance with an internal Fibre Channel interface and is automatically assigned and enabled.

An FCIP instance runs with a point-to-point connection to an FCIP instance on a peer SN 5428-2 Storage Router. Each FCIP instance requires one and only one peer.

Use this command to configure a peer destination name and IP address, using TCP/IP as the protocol type. When configured as a TCP client, the FCIP instance initiates the connection to the peer destination. The peer destination must be configured as a TCP server. The TCP server listens for the initial connection.



Note

The only functional difference between an FCIP instance configured as a TCP client and an FCIP instance configured as a TCP server is during the initial connection, which is initiated by the TCP client.

The destination IP address is the Gigabit Ethernet IP address of the FCIP instance running in the peer SN 5428-2 Storage Router.

TCP/IP connection protocol uses the FCIP standard and TCP flow control and error recovery algorithms. FCIP, using TCP connections, allows you to configure TCP receive and transmit window sizes.

**Note**

When configuring an FCIP instance, you must configure the network interface before you configure the peer destination and protocol.

Examples

The following example configures the FCIP instance named *fcip2* with a destination named *lucky2* at IP address *10.1.4.32*, using TCP/IP connection protocol. The FCIP instance is configured as a TCP client, and will initiate the TCP connection to the destination.

```
[SN5428-2A]# fcip fcip2 destination lucky2 tcpclient 10.1.4.32
```

Related Commands

Command	Description
fcip	Create an FCIP instance.
fcip destination config	Configure operational parameters for the named FCIP instance.
fcip networkif	Assign a Gigabit Ethernet interface and IP address to the named FCIP instance.
show fcip	Display configuration and operational information for the named FCIP instance.

fcip destination tcpserver

To add a peer destination to the named FCIP instance, with a connection type of TCP/IP, use the **fcip destination tcpserver** command. The named FCIP instance will listen for the TCP connection from the named destination.

fcip *name* **destination** *name* **tcpserver** *A.B.C.D*

Syntax Description	<i>name</i>	The name of the FCIP instance. Valid names are <i>fcip1</i> and <i>fcip2</i> .
	destination <i>name</i>	The name of the peer destination. Enter a maximum of 31 characters.
	<i>A.B.C.D</i>	The IP address of the peer destination. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The peer destination is the FCIP instance running in the partner SN 5428-2 Storage Router.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.3.1	This command was introduced.

Usage Guidelines Each FCIP instance requires three active elements:

- The *networkif* element assigns an interface and IP address for use by the FCIP peer.
- The *destination* element assigns the peer’s protocol and IP address.
- The device interface element associates the FCIP instance with an internal Fibre Channel interface and is automatically assigned and enabled.

An FCIP instance runs with a point-to-point connection to an FCIP instance on a peer SN 5428-2 Storage Router. Each FCIP instance requires one and only one peer.

Use this command to configure a peer destination name and IP address, using TCP/IP as the protocol type. When configured as a TCP server, the FCIP instance listens for the connection from the peer destination. The peer destination must be configured as a TCP client. The TCP client initiates the TCP initial TCP connection.



Note The only functional difference between an FCIP instance configured as a TCP client and an FCIP instance configured as a TCP server is during the initial connection, which is initiated by the TCP client.

The destination IP address is the Gigabit Ethernet IP address of the FCIP instance running in the peer SN 5428-2 Storage Router.

TCP/IP connection protocol uses the FCIP standard and TCP flow control and error recovery algorithms. FCIP, using TCP connections, allows you to configure TCP receive and transmit window sizes.

**Note**

When configuring an FCIP instance, you must configure the network interface before you configure the peer destination and protocol.

Examples

The following example configures the FCIP instance named *fcip1* with a destination named *dest1* at IP address *10.1.5.222*, using TCP/IP connection protocol. The FCIP instance is configured as a TCP server, and will listen for the TCP connection from the destination.

```
[SN5428-2A]# fcip fcip1 destination dest1 tcpserver 10.1.5.222
```

Related Commands

Command	Description
fcip	Create an FCIP instance.
fcip destination config	Configure operational parameters for the named FCIP instance.
fcip networkif	Assign a Gigabit Ethernet interface and IP address to the named FCIP instance.
show fcip	Display configuration and operational information for the named FCIP instance.

fcip enable

To start the named FCIP instance on this SN 5428-2 Storage Router, use the **fcip enable** command. To stop the named FCIP instance, use the **no** form of this command.

```
fcip {name | all} enable

no fcip {name | all} enable
```

Syntax Description	<i>name</i>	The name of the FCIP instance to be started. Valid names are <i>fcip1</i> and <i>fcip2</i> .
	all	Start all FCIP instances on this storage router.

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.3.1	This command was introduced.

Usage Guidelines

FCIP instances are automatically started by the storage router during the creation process and when the storage router is restarted. Use this command to manually control the running state of FCIP instances.

Use the **all** keyword to start all FCIP instances on the SN 5428-2. All instances previously stopped on this storage router will be restarted. This form of the command is always available; the only time the command is available for a named FCIP instance is when that FCIP instance has been previously stopped.

Examples

The following example starts the FCIP instance named *fcip2*. This instance must have been previously stopped.

```
[SN5428-2A] # fcip fcip2 enable
```

The following example stops all FCIP instances running on the storage router:

```
[SN5428-2A] # no fcip all enable
```


Related Commands	Command	Description
	<code>delete fcip</code>	Delete the named FCIP instance or the specified element of the FCIP instance.
	<code>fcip</code>	Create an FCIP instance.
	<code>show fcip</code>	Display configuration and operational information for the named FCIP instance.

fcip networkif

To assign a Gigabit Ethernet interface and IP address to the named FCIP instance, use the **fcip networkif** command. The specified interface provides IP connectivity between the FCIP instance and its peer destination.

```
fcip name networkif {A.B.C.D/bits | A.B.C.D/1.2.3.4} [secondary]
```

Syntax Description	<i>name</i>	Name of the FCIP instance to which you are adding the Gigabit Ethernet interface. Valid names are <i>fcip1</i> and <i>fcip2</i> .
	<i>A.B.C.D/bits</i>	The IP address of the named interface. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style. Note For the FCIP instance named <i>fcip1</i> , the IP address must be accessible from the Gigabit Ethernet interface, <i>ge1</i> . For the instance named <i>fcip2</i> , the IP address must be accessible from the interface <i>ge2</i> .
	<i>A.B.C.D/1.2.3.4</i>	The IP address of the named interface. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask.
	secondary	(Optional) Indicates the specified IP address is available from both Gigabit Ethernet interfaces. If the primary interface goes down and remains down for two seconds, the specified IP address will be moved to the secondary interface.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.3.1	This command was introduced.

Usage Guidelines

The specified interface IP address is configured as the destination IP address for the FCIP instance running in the peer SN 5428-2 Storage Router.

Each FCIP instance requires three active elements:

- The *networkif* element assigns an interface and IP address for use by the FCIP peer.
- The *destination* element assigns the peer’s protocol and IP address.
- The device interface element associates the FCIP instance with an internal Fibre Channel interface and is automatically assigned and enabled.

An FCIP instance runs with a point-to-point connection to an FCIP instance on a peer SN 5428-2 Storage Router. Each FCIP instance requires one and only one peer.

**Note**

Each FCIP instance must connect to a unique peer SN 5428-2 Storage Router. If you have two FCIP instances running in a single storage router, you cannot connect both instances to the same peer SN 5428-2 Storage Router.

Use this command to configure an IP address for the FCIP instance, to be used by the FCIP peer for IP connectivity. For the FCIP instance named *fcip1*, the IP address is automatically associated with the Gigabit Ethernet interface, *ge1*. For the FCIP instance named *fcip2*, the IP address is automatically associated with the Gigabit Ethernet interface, *ge2*.

When configuring an FCIP instance, you must configure the network interface before you configure the peer destination and protocol.

If the **secondary** keyword is used, both Gigabit Ethernet interfaces must be connected to the same network segment. If the primary interface goes down and remains down for two seconds, the IP address will be moved to the secondary interface.

**Note**

If you configure a Gigabit Ethernet IP address with a secondary interface, all Gigabit Ethernet IP addresses on the same subnet must also be configured with the same secondary interface.

You can configure two FCIP instances on a single storage router to use the same network interface. You must fully configure one FCIP instance, and then configure a second FCIP instance without configuring a network interface. The second FCIP instance will use the same network interface as configured for the first instance. The two FCIP instances should use different connection protocols, or if both are configured as TCP servers, each FCIP instance must use a unique TCP port number.

Examples

The following command adds the IP address 10.1.10.128/24, to the FCIP instance named *fcip2*. This IP address will automatically be associated with the Gigabit Ethernet interface, *ge2*.

```
[SN5428-2A]# fcip fcip2 networkif 10.1.10.128/24
```

The following command adds the IP address 10.1.30.128, with a netmask of 255.255.255.0, to the FCIP instance *fcip1*. This IP address is automatically associated with the Gigabit Ethernet interface, *ge1*. If the primary interface is not available, the IP address will be moved to the secondary Gigabit Ethernet interface, *ge2*. The Gigabit Ethernet interfaces must be connected to the same network.

```
[SN5428-2A]# fcip fcip1 networkif 10.1.30.128/255.255.255.0 secondary
```

The following set of commands configures the FCIP instance named *fcip1*, adds the network IP address 10.1.40.42/24, and configures the destination, *dest1*, with a TCP client connection type. The second FCIP instance, *fcip2*, is configured with a destination named *dest2* and a TCP server connection type. Both FCIP instances will use the 10.1.40.42/24 network interface.

```
[SN5428-2A]#fcip fcip1
*[SN5428-2A] fcip fcip1 networkif 10.1.40.42/24
*[SN5428-2A] fcip fcip1 destination dest1 tcpclient 10.1.1.144
*[SN5428-2A] fcip fcip2
*[SN5428-2A] fcip fcip2 destination dest2 tcpserver 10.1.5.73
```


Related Commands	Command	Description
	fcip	Create an FCIP instance.
	fcip destination config	Configure operational parameters for the named FCIP instance.
	fcip destination raw	Add a peer destination to the named FCIP instance, with a connection type of raw IP.
	fcip destination tcpclient	Add a peer destination to the named FCIP instance, with a connection type of TCP/IP. The named FCIP instance initiates the TCP connection.
	fcip destination tcpserver	Add a peer destination to the named FCIP instance, with a connection type of TCP/IP. The named FCIP instance listens for the TCP connection from the named destination.
	show fcip	Display configuration and operational information for the named FCIP instance.

fcswitch beacon enable

To enable all Fibre Channel port Logged-In (LOG) LEDs to flash, use the **fcswitch beacon enable** command. To disable LOG LED flashing, use the **no** form of this command.

fcswitch beacon enable

no fcswitch beacon enable

Syntax Description This command has no arguments or keywords.

Defaults Beacon flashing is disabled, by default. See the *SN 5428-2 Storage Router Hardware Installation Guide* for default LOG LED indication descriptions.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use this command to assist in locating a physical unit. This command is primarily used for troubleshooting purposes.

Examples The following example causes all Fibre Channel port LOG LEDs on the storage router to flash:

```
[SN5428-2A] # fcswitch beacon enable
```

Related Commands	Command	Description
	show debug fcswitch	Display internal Fibre Channel interface parameters.
	show fcswitch	Display global configuration information for storage router FC interfaces.

fcswitch devlog

To specify the logging parameters for the SN 5428-2 Storage Router integrated Fibre Channel (FC) switch component development log file, use the **fcswitch devlog** command.

fcswitch devlog components *component1* [*component2...*]

fcswitch devlog level *notification-level*

Syntax Description	components	At least one of the components described in Table 12-6 .
	<i>component1</i> <i>[component2...]</i>	
	level <i>notification-level</i>	Limit logging to messages of a specified level or lower. See Table 12-7 in the Usage Guidelines section for a list of valid names that can be used for the <i>notification-level</i> argument.

Defaults	No components or notification level are configured. Development logging for the SN 5428-2 Storage Router integrated FC switch component is disabled.
-----------------	--

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	The fcswitch devlog command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.
-------------------------	---

After logging is enabled, use this command to limit the amount of information recorded in the switch development log by component and by notification level. To stop all logging for all components, set the notification level to **none**. Use the **fcswitch devlog enable** command to enable development logging.

Table 12-6 fcswitch devlog components

Component	Description
Cmon	Monitors internal chassis components and applications.
Diag	Handles online testing and other diagnostic tasks.
Ds	Data services repository for all switch data.
Fc2	Class 2 frame handler.
MgmtApp	Manages the user interface and internal configuration for the switch.
PortApp	Manages the switch ports.

Table 12-6 *fcswitch devlog components (continued)*

Component	Description
Swb	Software bus internal process communications mechanism.
Util	Utility message interpreter for handling legacy user interfaces.

Table 12-7 *fcswitch devlog notification-level*

Notification Level	Description
Critical	Log all messages from the selected components (critical, warning and informational).
Warn	Log all warning and informational messages for the selected components.
Info	Log informational messages only for the selected components.
None	Log no messages. This setting stops switch development logging.

Examples

The following example limits the switch development log file to informational messages only from the management application and the class 2 frame handler:

```
[SN5428-2A] # fcswitch devlog components MgmtApp Fc2
[SN5428-2A] # fcswitch devlog level info
```

The following example stops all switch devlog logging:

```
[SN5428-2A] # fcswitch devlog level none
```

Related Commands

Command	Description
clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
fcswitch devlog enable	Enable development logging for the integrated FC switch component.
fcswitch log interface	Restrict the integrated FC switch logging to information related to a specific FC interface.
show debug fcswitch	Display internal FC interface parameters, including switch log entries.

fcswitch devlog enable

To start development logging for the SN 5428-2 Storage Router integrated Fibre Channel (FC) switch component, use the **fcswitch devlog enable** command. To stop development logging, use the **no** form of this command.

fcswitch devlog enable

no fcswitch devlog enable

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	Development logging is stopped.
-----------------	---------------------------------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	The fcswitch devlog enable command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.
-------------------------	--

Examples	The following example starts development logging for the FC switch component and limits the switch development log file to informational messages only from the management application and the class 2 frame handler:
-----------------	---

```
[SN5428-2A] # fcswitch devlog components MgmtApp Fc2
[SN5428-2A] # fcswitch devlog level info
[SN5428-2A] # fcswitch devlog enable
```

Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	fcswitch devlog	Specify logging parameters for the switch development log file.
	fcswitch log interface	Restrict the integrated FC switch logging to information related to a specific FC interface.
	show debug fcswitch	Display internal FC interface parameters, including switch log entries.

fcswitch diag

To set all Fibre Channel (FC) interfaces into diagnostic mode for testing purposes, use the **fcswitch diag** command.

fcswitch diag

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to change all FC interfaces to diagnostic mode prior to performing internal or external loopback testing on individual FC interfaces.
	<ul style="list-style-type: none">• Use the fcswitch enable command to reenable all FC interfaces. An FC interface must be enabled to run online loopback tests or to allow access to storage targets.• Use the no fcswitch enable command to disable all FC interfaces. When you are ready to allow access to the storage targets, you can enable all FC interfaces at once via the fcswitch enable command, or enable individual interfaces via the interface fc? enable command.

Examples	The following example sets all FC interfaces into a diagnostic state and then performs an internal loopback test on the FC interface named <i>fc6</i> :
-----------------	---

<pre>[SN5428-2A] # fcswitch diag [SN5428-2A] # interface fc6 loopback internal</pre>
--

Related Commands	Command	Description
	fcswitch enable	Enable all FC interfaces.
	interface fc? diag	Set the named FC interface into diagnostic mode for testing purposes.
	interface fc? enable	Enable the named FC interface.
	interface fc? loopback	Initiate a loopback test on the named FC interface.
	show fcswitch	Display global configuration information for storage router FC interfaces.

fcswitch domainid

To set the SN 5428-2 Storage Router’s domain ID for switched zoned fabric to a unique value, and to prevent the FC fabric from changing that domain ID, use the **fcswitch domainid** command. To disable the lock and allow the domain ID to be changed by the switched zoned fabric, use the **no** form of this command.

fcswitch domainid {*domain-id*} [**force**]

fcswitch domainid lock enable

no fcswitch domainid lock enable

Syntax Description

<i>domain-id</i>	The domain identification number associated with the storage router.
force	(Optional) Suppress warning prompts and messages.
lock enable	Keywords used to disallow changes to the domain ID from the switched zoned fabric.

Defaults

The default domain ID for fabric zoning is 1. The domain ID can be changed by the switched zoned fabric, by default.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to set the SN 5428-2 Storage Router’s domain identification number for switched zoned fabric to a unique value or to prevent changes to that value by the zoned fabric. Domain IDs allow fabrics to be segmented into different areas.

Domain IDs must be unique among all switch elements within a fabric. If there is a domain ID conflict, the expansion ports (ports operating as E_Ports) on the two conflicting elements are disabled, isolating the Interswitch Link (ISL).

If you are planning to connect to a switched zoned fabric via one or more FC interfaces, complete the appropriate zoning configuration for the storage router, as described in [Chapter 5, “Configuring Fibre Channel Interfaces.”](#)



Note

Changing the domain ID in an operational fabric may cause traffic disruption. All ports operating as E_Ports should be inactive or disabled prior to changing the domain ID.

Examples

The following example sets the switched zoned fabric domain ID for the storage router to 42:

```
[SN5428-2A]# fcswitch domainid 42
*** Warning: Changing domain ID in an operational fabric will cause traffic disruption
Do you want to continue? [(yes/no (no))] yes
```

The following example sets the switched zoned fabric domain ID for the storage router to 5 and enables the lock, which prevents the domain ID from being changed by the zoned fabric.

```
[SN5428-2A]# fcswitch domainid 5
*** Warning: Changing domain ID in an operational fabric will cause traffic disruption
Do you want to continue? [(yes/no (no))] yes
[SN5428-2A]# fcswitch domainid lock enable
```

Related Commands

Command	Description
fcswitch enable	Enable all FC interfaces.
fcswitch interop-credit	Set the data buffer credit capacity for all FC ports.
fcswitch zoning autosave	Configure the storage router to participate in FC switched zones.
fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
fcswitch zoning merge	Set zoning merge compliance.
interface fc? diag	Set the named FC interface into diagnostic mode for testing purposes.
interface fc? enable	Enable the named FC interface.
interface fc? loopback	Initiate a loopback test on the named FC interface.
show fcswitch	Display global configuration information for storage router FC interfaces.
show fcswitch eport	Display FSPF protocol information.

fcs switch dstov

To specify the amount of time the storage router is to wait for Fibre Channel (FC) Distributed Services, use the **fcs switch dstov** command.

fcs switch dstov {*nn* | **default**}

Syntax Description

<i>nn</i>	The Distributed Services timeout value, in milliseconds.
default	Keyword, indicating the storage router is to wait 5000 milliseconds for Fibre Channel Distributed Services.

Defaults

The default Distributed Services timeout value is 5000 milliseconds.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to specify the length of time the storage router should wait for FC Distributed Services, such as the Management Server or Name Server, before returning an error.

Use the **default** keyword to return the Distributed Services timeout value to 5000 milliseconds.

Examples

The following example sets the Distributed Services timeout value to 7500 milliseconds:

```
[SN5428-2A] # fcs switch dstov 7500
```

The following example resets the Distributed Services timeout value to the default of 5000 milliseconds:

```
[SN5428-2A] # fcs switch dstov default
```

Related Commands

Command	Description
fcs switch edtov	Specify an error detect timeout value for all Fibre Channel interfaces.
fcs switch enable	Enable all FC interfaces.
fcs switch fstov	Specify the fabric stability timeout value.
fcs switch ratov	Specify a Fibre Channel resource allocation timeout value for the storage router.
show fcs switch	Display global configuration information for storage router FC interfaces.

fcswitch edtov

To specify an error detect timeout value for all Fibre Channel (FC) interfaces, use the **fcswitch edtov** command.

fcswitch edtov {*nn* | **default**}

Syntax Description

<i>nn</i>	The amount of time a port is to wait for errors to clear, in milliseconds.
default	Keyword, indicating the port is to wait 2000 milliseconds for errors to clear.

Defaults

The default error detect timeout value is 2000 milliseconds.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The error detect timeout value is the amount of time the FC port is to wait for all errors to clear. This value applies to all FC interfaces in the storage router.

Error detect timeout values should be the same for all SN 5428-2 Storage Routers or switches in the fabric.

Examples

The following example sets the error detect timeout value to 4000 milliseconds:

```
[SN5428-2A] # fcswitch edtov 4000
```

The following example resets the error detect timeout value to the default of 2000 milliseconds:

```
[SN5428-2A] # fcswitch edtov default
```

Related Commands

Command	Description
fcswitch dstov	Specify the amount of time the storage router is to wait for Fibre Channel Distributed Services.
fcswitch enable	Enable all FC interfaces.
fcswitch fstov	Specify the fabric stability timeout value.
fcswitch ratov	Specify a Fibre Channel resource allocation timeout value for the storage router.
show fcswitch	Display global configuration information for storage router FC interfaces.

fcswitch enable

To enable all Fibre Channel (FC) interfaces, use the **fcswitch enable** command. To disable all FC interfaces, use the **no** form of this command.

- fcswitch enable**
- no fcswitch enable**

Syntax Description This command has no arguments or keywords.

Defaults All FC interfaces are enabled, by default.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines An FC interface must be enabled to allow access to storage targets or perform online loopback testing. Use this command to enable all FC interfaces at one time.

If you experience problems with FC storage, use the **no** form of this command to quickly disable all FC interfaces at once.

Examples The following example enables all FC interfaces and then performs an online loopback test for the FC interface named *fc6*:

```
[SN5428-2A] # fcswitch enable
[SN5428-2A] # interface fc6 loopback online
```

The following example disables all FC interfaces.

```
[SN5428-2A] # no fcswitch enable
```


Related Commands	Command	Description
	fcswitch diag	Set all FC interfaces into diagnostic mode for testing purposes.
	interface fc? diag	Set the named FC interface into diagnostic mode for testing purposes.
	interface fc? enable	Enable the named FC interface.
	interface fc? loopback	Initiate a loopback test on the named FC interface.
	show fcswitch	Display global configuration information for storage router FC interfaces.
	show fcswitch eport	Display FSPF protocol information.

fcs switch fstov

To specify the fabric services timeout value, use the **fcs switch fstov** command.

fcs switch fstov {*nn* | **default**}

Syntax Description	<i>nn</i>	The amount of time the storage router is to wait for fabric services, in milliseconds.
	default	Keyword, indicating the storage router will wait for 1000 milliseconds for fabric services.

Defaults The default fabric stability timeout value is 1000 milliseconds.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use this command to specify the number of milliseconds the storage router will wait for fabric services.

Examples The following example sets the fabric services timeout value to 5000 milliseconds:

```
[SN5428-2A] # fcs switch fstov 5000
```

The following example resets the fabric services timeout value to the default of 1000 milliseconds:

```
[SN5428-2A] # fcs switch fstov default
```

Related Commands	Command	Description
	fcs switch dstov	Specify the amount of time the storage router is to wait for Fibre Channel Distributed Services.
	fcs switch edtov	Specify an error detect timeout value for all Fibre Channel interfaces.
	fcs switch enable	Enable all FC interfaces.
	fcs switch ratov	Specify a Fibre Channel resource allocation timeout value for the storage router.
	show fcs switch	Display global configuration information for storage router FC interfaces.

fcswitch interop-credit

To set the buffer-to-buffer credit value for all Fibre Channel (FC) ports, use the **fcswitch interop-credit** command.

fcswitch interop-credit *credit*

Syntax Description

<i>credit</i>	The data buffer credit capacity, also known as the buffer-to-buffer credit value. The <i>credit</i> variable is an integer between 0 and 255 inclusive. The default value is 12.
---------------	--

Defaults

The data buffer credit capacity is 12, by default.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to set the data buffer credit capacity for all the storage router FC ports. The port buffer credit is used to determine how many maximum sized frames can be sent to a recipient before the sending port must wait for an acknowledgement. When the acknowledgement is received, the sending port can continue by sending the next frame. Port buffer credits are required when buffer-to-buffer flow control is in use. Buffer-to-buffer flow control occurs between directly connected FC ports.

The data buffer credit capacity must be the same for all switches across the fabric, and should be set to the lowest system-wide setting.

Examples

The following example sets the data buffer credit capacity to 15:

```
[SN5428-2A] # fcswitch interop-credit 15
```


Related Commands	Command	Description
	fcswitch domainid	Set the domain ID for the storage router, to be used for FC switched fabric zoning.
	fcswitch enable	Enable all FC interfaces.
	fcswitch zoning autosave	Configure the storage router to participate in FC switched zones.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	fcswitch zoning merge	Set zoning merge compliance.
	interface fc? diag	Set the named FC interface into diagnostic mode for testing purposes.
	interface fc? enable	Enable the named FC interface.
	interface fc? loopback	Initiate a loopback test on the named FC interface.
	show fcswitch	Display global configuration information for storage router FC interfaces.

fcswitch log interface

To restrict the SN 5428-2 Storage Router integrated Fibre Channel (FC) switch logging to information related to a specific FC interface, use the **fcswitch log interface** command.

fcswitch log interface {*if-name* | **default**}

Syntax Description	<i>if-name</i>	The name of the FC interface for which you are setting this parameter. Valid values are fc1 through fc8. When you type the interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
	default	Enable logging for all FC interfaces.
Defaults	None.	
Command Modes	Administrator.	
Command History	Release	Modification
	3.2.1	This command was introduced.
Usage Guidelines	The fcswitch log interface command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.	
Examples	The following example restricts logging for the integrated FC switch to information associated with <i>fc3</i> : [SN5428-2A] # fcswitch log interface fc3	
Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	fcswitch devlog	Specify logging parameters for the switch development log file.
	fcswitch devlog enable	Enable development logging for the integrated FC switch component
	fcswitch syslog	Specify logging parameters for the switch system log file.
	fcswitch syslog enable	Enable system logging for the integrated FC switch component.
	show debug fcswitch	Display internal FC interface parameters, including switch log entries.

fcswitch ratov

To specify a Fibre Channel (FC) resource allocation timeout value for the storage router, use the **fcswitch ratov** command.

fcswitch ratov {*nn* | **default**}

Syntax Description

<i>nn</i>	The amount of time the storage router is to wait to allow two FC ports to allocate enough resources to establish a link.
default	Keyword, indicating the storage router is to wait up to 10000 milliseconds to allow two FC ports to allocate enough resources to establish a link.

Defaults

The default resource allocation timeout value is 10000 milliseconds.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The resource allocation timeout value is the amount of time the storage router is to wait to allow two FC ports to allocate sufficient resources to establish a link.

Resource allocation timeout values should be the same for all SN 5428-2 Storage Routers or switches in the fabric.

Examples

The following example sets the resource allocation timeout value to 9000 milliseconds:

```
[SN5428-2A] # fcswitch ratov 9000
```

The following example resets the resource allocation timeout value to the default of 10000 milliseconds:

```
[SN5428-2A] # fcswitch ratov default
```

Related Commands

Command	Description
fcswitch dstov	Specify the amount of time the storage router is to wait for Fibre Channel Distributed Services.
fcswitch edtov	Specify an error detect timeout value for all Fibre Channel interfaces.
fcswitch enable	Enable all FC interfaces.
fcswitch fstov	Specify the fabric stability timeout value.
show fcswitch	Display global configuration information for storage router FC interfaces.

fcswitch syslog

To specify the logging parameters for the SN 5428-2 Storage Router integrated Fibre Channel (FC) switch component system log file, use the **fcswitch syslog** command.

fcswitch syslog components *component1* [*component2...*]

fcswitch syslog level *notification-level*

Syntax Description

components <i>component1</i> [<i>component2...</i>]	At least one of the components described in Table 12-8 .
level <i>notification-level</i>	Limit logging to messages of a specified level or lower. See Table 12-9 in the Usage Guidelines section for a list of valid names that can be used for the <i>notification-level</i> argument.

Defaults

All components log information into the SN 5428-2 Storage Router integrated FC switch component system log, by default. The default notification level is *critical*.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to limit the amount of information recorded in the switch system log by component and by notification level. To stop all logging for all components, set the notification level to **none**.

Table 12-8 fcswitch syslog components

Component	Description
Blade	Monitors modular circuit boards.
Chassis	Monitors chassis hardware components.
Eport	Monitors all Fibre Channel interfaces where the port is operating as an expansion port (E_Port).
NameServer	Monitors name server events.
MgmtServer	Monitors management server status.
Other	Monitors miscellaneous events.
Port	Monitors all port events.
Switch	Monitors switch management events.
Zoning	Monitors zoning conflict events.

Table 12-9 *fcswitch syslog notification level*

Notification Level	Description
Critical	Log all messages from the selected components (critical, warning and informational).
Warn	Log all warning and informational messages for the selected components.
Info	Log informational messages only for the selected components.
None	Log no messages. This setting stops switch system logging.

Examples

The following example limits the switch system log file to informational messages only for name server, management server, port and switch management events:

```
[SN5428-2A] # fcswitch syslog components NameServer MgmtServer Port Switch
[SN5428-2A] # fcswitch syslog level info
```

The following example stops all switch syslog logging:

```
[SN5428-2A] # fcswitch syslog level none
```

Related Commands

Command	Description
clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
fcswitch log interface	Restrict the integrated FC switch logging to information related to a specific FC interface.
fcswitch syslog enable	Enable system logging for the integrated FC switch component.
show debug fcswitch	Display internal FC interface parameters, including switch log entries.

fcswitch syslog enable

To start system logging for the SN 5428-2 Storage Router integrated Fibre Channel (FC) switch component, use the **fcswitch syslog enable** command. To stop system logging, use the **no** form of this command.

fcswitch syslog enable

no fcswitch syslog enable

Syntax Description This command has no arguments or keywords.

Defaults System logging for the integrated FC switch component is started, by default.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines The **fcswitch syslog enable** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

Examples The following example stops system logging for the integrated FC switch component. When system logging is started, logging will continue based on the existing component and notification level settings.

```
[SN5428-2A] # no fcswitch syslog enable
```

Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	fcswitch log interface	Restrict the integrated FC switch logging to information related to a specific FC interface.
	fcswitch syslog	Specify logging parameters for the switch system log file.
	show debug fcswitch	Display internal FC interface parameters, including switch log entries.

fcswitch zoning autosave

To enable the SN 5428-2 Storage Router to automatically save zoning changes received from switches in the fabric, use the **fcswitch zoning autosave** command. To prevent the storage router from saving zoning changes, use the **no** form of this command.

- fcswitch zoning autosave enable**
- no fcswitch zoning autosave enable**

Syntax Description	autosave enable	Enables the storage router to save zoning changes received from switches in the fabric to non-volatile memory. This is the default.
--------------------	------------------------	---

Defaults	The storage router saves zoning changes by default.
----------	---

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	By default, the SN 5428-2 Storage Router can merge into existing FC switched fabric zones and participate in the zoning. Use the no form of this command, in conjunction with the fcswitch domainid command with the lock keyword to prevent the storage router from participating in FC switched fabric zones.
------------------	--

Examples	<p>The following example prevents the storage router from participating in FC switched fabric zones. The first command prevents the storage router from saving zoning changes received from switches in the fabric, and the second command locks the domain ID, preventing the FC switched fabric from making changes to that value.</p> <pre>[SN5428-2A] # no fcswitch zoning autosave enable [SN5428-2A] # fcswitch domainid lock enable</pre>
----------	--

Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	fcswitch domainid	Set the domain ID for the storage router, to be used for FC switched fabric zoning.
	fcswitch enable	Enable all FC interfaces.
	fcswitch interop-credit	Set the data buffer credit capacity for all FC ports.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	fcswitch zoning merge	Set zoning merge compliance.
	interface fc? diag	Set the named FC interface into diagnostic mode for testing purposes.
	interface fc? enable	Enable the named FC interface.
	interface fc? loopback	Initiate a loopback test on the named FC interface.
	show fcswitch	Display global configuration information for storage router FC interfaces.
	zone	Create a Fibre Channel fabric zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset enable	Activate a zone set.

fcswitch zoning default

To select the level of communication between the storage router and devices in the fabric when there is no active zone set, use the **fcswitch zoning default** command.

fcswitch zoning default {all | none}

Syntax Description	default all	Enables the storage router to communicate with all switches and other devices in the fabric when there is no active zone set. This is the default.
	default none	When there is no active zone set, the storage router cannot communicate with any other switch or device in the fabric.

Defaults	If there is no active zone set, the storage router can communicate with all switches and other devices in the fabric, by default.
----------	---

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	<p>By default, the SN 5428-2 Storage Router can merge into existing FC switched fabric zones and participate in the zoning. Use this command to isolate the storage router and prevent communication with any switch or other device in the fabric, if there is no active zone set.</p> <p>Before changing the default behavior, disconnect any ISL links to other fabric entities to prevent unintended disruption of fabric traffic.</p>
------------------	--

Examples	<p>The following example prevents the storage router from communicating with switches and all other devices in the fabric, if there is no active zone set:</p> <pre>[SN5428-2A] # fcswitch zoning default none</pre>
----------	--

Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	fcswitch domainid	Set the domain ID for the storage router, to be used for FC switched fabric zoning.
	fcswitch enable	Enable all FC interfaces.
	fcswitch interop-credit	Set the data buffer credit capacity for all FC ports.
	fcswitch zoning autosave	Enable the SN 5428-2 Storage Router to save zoning changes received from switches in the fabric.
	fcswitch zoning merge	Set zoning merge compliance.
	interface fc? diag	Set the named FC interface into diagnostic mode for testing purposes.
	interface fc? enable	Enable the named FC interface.
	interface fc? loopback	Initiate a loopback test on the named FC interface.
	show fcswitch	Display global configuration information for storage router FC interfaces.
	zone	Create a Fibre Channel fabric zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset enable	Activate a zone set.

fcswitch zoning merge

To set zoning merge compliance, use the **fcswitch zoning merge** command.

fcswitch zoning merge sw2

Syntax Description	sw2	Indicates the fabric includes only FC-SW-2 compliant switches. A merge may only occur of active zoning information, ensuring all switches have identical active zone sets. This is the default.
--------------------	-----	---

Defaults	The SN 5428-2 Storage Router is FC-SW-2 compliant, and is configured to participate in a fabric with only FC-SW-2 compliant switches by default.	
----------	--	--

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	By default, the SN 5428-2 Storage Router can merge into existing FC switched fabric zones and participate in the zoning. All switches in a fabric should be set to the same merge mode to prevent switches from becoming isolated from each other. By default, the storage router supports the FC-SW-2 compliant merge mode.	
------------------	--	--

Examples	The following example sets the merge mode for participation in a fabric with FC-SW-2 compliant switches: [SN5428-2A] # fcswitch zoning merge sw2	
----------	--	--

Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	fcswitch domainid	Set the domain ID for the storage router, to be used for FC switched fabric zoning.
	fcswitch enable	Enable all FC interfaces.
	fcswitch interop-credit	Set the data buffer credit capacity for all FC ports.
	fcswitch zoning autosave	Enable the SN 5428-2 Storage Router to save zoning changes received from switches in the fabric.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	interface fc? diag	Set the named FC interface into diagnostic mode for testing purposes.
	interface fc? enable	Enable the named FC interface.
	interface fc? loopback	Initiate a loopback test on the named FC interface.
	show fcswitch	Display global configuration information for storage router FC interfaces.
	zone	Create a Fibre Channel fabric zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset enable	Activate a zone set.

halt

To prepare the storage router to be powered down, issue the **halt** command.

halt [**force**] [**fast**]

Syntax Description	force	(Optional) Force an immediate halt of the SN 5428-2 Storage Router.
	fast	(Optional) Bypass hardware diagnostics when the storage router is next restarted.

Defaults	If there are unsaved configuration changes when the command is issued, the default is to save all changes before halting. If the command is issued with the optional force keyword, any unsaved configuration changes are discarded.
----------	---

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	The halt command prepares the SN 5428-2 Storage Router file system to be powered down. If the storage router is participating in a cluster, the halt command will cause any SCSI routing instances running on this SN 5428-2 to failover to another storage router in the cluster.
	If the halt command is issued with no keywords and there are unsaved changes to the current configuration, you are prompted to save or discard the changes.
	Use the force keyword to cause an immediate halt of the storage router, discarding any unsaved configuration changes. Append the optional fast keyword to bypass diagnostics when the storage router is restarted.
	When the halt command completes, the storage router displays the following system prompt: [HALTED] #
	The storage router can be safely powered down when the HALTED system prompt appears. The only CLI command that can be issued from the storage router at the HALTED system prompt is the reboot command.



Note

When the storage router is restarted, the cluster determines any SCSI routing instances that should start on the SN 5428-2. If the storage router is identified as the preferred storage router for any SCSI routing instance (via the **scsirouter primary** command), that instance will start running on the SN 5428-2 (assuming targets and critical resources are available).

Examples

The following prompt is received if you issue a **halt** command (without the **force** keyword) when the storage router has unsaved configuration changes.

```
[SN5428-2A]# halt
*** Warning: This will halt the system.
Do you want to continue? [yes/no (no)] yes

Changes have been made to the current configuration of the system which
have not been saved.
yes    - all of the configuration data will be saved,
no     - modifications to the configuration data will not be saved.

Save ALL configuration data? [yes/no (yes)] no
Halting system.....!
[HALTED]#
```

The following example halts the SN 5428-2 Storage Router (after prompting you to save any unsaved configuration changes). Diagnostics will be bypassed when the storage router is restarted.

```
[SN5428-2A]# halt fast
```

Related Commands

Command	Description
reboot	Cause the SN 5428-2 Storage Router to shut down and then restart.

help

To display information on how to use the CLI, issue the **help** command.

help

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines The **help** command displays information about the various CLI commands that can be issued, based on the mode currently in use. The **help** command also displays information about the special keys that can be used in the CLI.

Examples The following example shows the special key information returned as a result of the **help** command:

```
[SN5428-2A]# help
```

```
Special keys:
?                list choices
Backspace       delete character backward
Tab             complete current word
Ctrl-A          go to beginning of line
Ctrl-B or Arrow Left go backward one character
Ctrl-D          delete character
Ctrl-E          go to end of line
Ctrl-F or Arrow Right go forward one character
Ctrl-K          delete from current position to end of line
Ctrl-N or Arrow Down go to next line in history buffer
Ctrl-P or Arrow Up go to previous line in history buffer
Ctrl-T          transpose current character and previous character
Ctrl-U          delete line
Ctrl-W          delete previous word
```

Related Commands	Command	Description
	enable	Enter Administrator mode.
	exit	Leave Administrator mode and enter Monitor mode.

hostname

To specify a new system name for the SN 5428-2 Storage Router, use the **hostname** command. The storage router is recognized by this name through the management interface.

This command takes effect immediately, and the new system name is automatically integrated into the prompt string.

hostname *sysname*

Syntax Description

<i>sysname</i>	The name of the storage router. This may be the fully qualified domain name. Maximum length is 19 characters. The name cannot contain blanks, white space, or control characters.
----------------	---

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The SN 5428-2 Storage Router must have a system name, which is assigned to the storage router during initial configuration. Use this command to change the system name.

If you wish to enable network management on the storage router using the facilities of a Domain Name Server (DNS), you must make the storage router system name and IP address known to the DNS. Use the system name specified in this command.

Examples

The following example changes the storage router name to *sn5428-2lab1*.

```
[SN5428-2A] # hostname sn5428-2lab1
```

Related Commands

Command	Description
save all	Save all configuration information.
save system	Save selected system configuration information.
show system	Display selected system information, including system name.

interface fc? al-fairness

To enable the fairness algorithm (loop priority) on the named Fibre Channel (FC) interface, use the **interface fc? al-fairness** command. To disable the fairness algorithm on the named FC interface, use the **no** form of this command.

interface fc? al-fairness enable

no interface fc? al-fairness enable

Syntax Description

<i>fc?</i>	The name of the FC interface for which you are setting this parameter. Valid values are fc1 through fc8. When you type the interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
enable	Keyword, required to enable the fairness algorithm on the named FC interface.

Defaults

The fairness algorithm is disabled on all FC interfaces by default, allowing the switch to have priority.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

When the fairness algorithm is not enabled for a specific FC interface, the switch receives priority. Use this command to enable the fairness algorithm for the named interface, removing the switch priority for that interface.



Note

All storage routers in a cluster should be configured with the same interface-specific parameters, allowing failover of SCSI routing instances to provide consistent performance characteristics.

Examples

The following example enables the fairness algorithm on the FC interface named *fc6*:

```
[SN5428-2A] # interface fc6 al-fairness enable
```

The following example disables the fairness algorithm on the FC interface named *fc3*. The switch receives priority for traffic on this interface.

```
[SN5428-2A] # no interface fc3 al-fairness enable
```


Related Commands

Command	Description
interface fc? default	Return the named FC interface to its default operational characteristics.
interface fc? fan-enable	Enable Fabric Address Notification (FAN) on the named FC interface.
interface fc? linkspeed	Set the transfer rate for the named FC interface.
interface fc? mfs-bundle	Enable Multi-Frame Sequence bundling for the named FC interface.
interface fc? ms-enable	Enable GS-3 management server commands for the specified FC interface.
interface fc? type	Set the port type for the named FC interface.
show interface	Display operational and configuration information for the specified interface or all interfaces.

interface fc? default

To return the named Fibre Channel (FC) interface to its default operational characteristics, use the **interface fc? default** command.

interface *fc?* default

Syntax Description	<i>fc?</i>	The name of the FC interface to be returned to its default operational characteristics. Valid values are fc1 through fc8. When you type the interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
--------------------	------------	---

Defaults	<p>The following are the default operational characteristics for the Fibre Channel interface:</p> <ul style="list-style-type: none"> • fairness algorithm is disabled (switch has priority) • Fabric Address Notification (FAN) is enabled • transfer rate is automatically negotiated (linkspeed auto) • Multi-Frame sequence bundling is enabled • GS-3 management server commands are enabled • port type is generic loop, indicating the port can function as either a fabric loop port (FL_Port), an expansion port (E_Port) or a fabric port (F_Port) • credit extension is not enabled (ext-credit is 0) 	
----------	--	--

Command Modes	Administrator.	
---------------	----------------	--

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	<p>Use this command to quickly reset the named FC interface to its default operational characteristics. The results of this command are the same as if each of the following commands were issued for the same named FC interface:</p> <ul style="list-style-type: none"> • no interface fc? al-fairness enable • interface fc? ext-credit 0 • interface fc? fan-enable enable • interface fc? linkspeed auto • interface fc? mfs-bundle enable timeout 10 • interface fc? ms-enable enable • interface fc? type gl-port 	
------------------	--	--


Note

All storage routers in a cluster should be configured with the same interface-specific parameters, allowing failover of SCSI routing instances to provide consistent performance characteristics.

Examples

The following example returns the operational characteristics to their default settings for the FC interface named *fc6*:

```
[SN5428-2A] # interface fc6 default
```

Related Commands

Command	Description
interface fc? al-fairness	Enable the fairness algorithm on the named FC interface.
interface fc? fan-enable	Enable Fabric Address Notification (FAN) on the named FC interface.
interface fc? linkspeed	Set the transfer rate for the named FC interface.
interface fc? mfs-bundle	Enable Multi-Frame Sequence bundling for the named FC interface.
interface fc? ms-enable	Enable GS-3 management server commands for the specified FC interface.
interface fc? type	Set the port type for the named FC interface.
show interface	Display operational and configuration information for the specified interface or all interfaces.

interface fc? diag

To set the named Fibre Channel (FC) interface into diagnostic mode for testing purposes, use the **interface fc? diag** command.

interface *fc?* diag

Syntax Description	<i>fc?</i>	The name of the FC interface to be placed into diagnostic mode. Valid values are fc1 through fc8. When you type the interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
--------------------	------------	---

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	<p>Use this command to change the named FC interface to diagnostic mode prior to performing an internal or external loopback test.</p> <ul style="list-style-type: none">• Use the interface fc? enable command to reenable the FC interface. An FC interface must be enabled to run an online loopback test, or to allow access to storage targets.• Use the no interface fc? enable command to disable the FC interface. When you are ready to allow access to the storage targets, you can enable all FC interfaces at once via the interface fc enable command, or enable individual interfaces via the interface fc? enable command.
------------------	--

Examples	<p>The following example sets the FC interface <i>fc6</i> into a diagnostic state and then performs an internal loopback test:</p> <pre>[SN5428-2A] # interface fc6 diag [SN5428-2A] # interface fc6 loopback internal</pre>
----------	--

Related Commands	Command	Description
	fcswitch diag	Set all FC interfaces into diagnostic mode for testing purposes.
	fcswitch enable	Enable all FC interfaces.
	interface fc? enable	Enable the named FC interface.
	interface fc? loopback	Initiate a loopback test on the named FC interface.
	interface fc? reset	Disable and then enable the specified FC interface.
	show fcswitch	Display global configuration information for storage router FC interfaces.

interface fc? enable

To enable the named Fibre Channel (FC) interface, use the **interface fc? enable** command. To disable the named FC interface, use the **no** form of this command.

```
interface fc? enable

no interface fc? enable
```

Syntax Description	fc?	The name of the FC interface to be enabled. Valid values are fc1 through fc8. When you type the interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
--------------------	-----	---

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

An FC interface must be enabled to allow access to storage targets or perform online loopback testing. Use this command to enable an individual FC interface.

If you experience a problem with the FC interface or a specific storage resource, use the **no** form of this command to disable the named FC interface.

Examples

The following example enables the FC interface *fc6* and then performs an online loopback test:

```
[SN5428-2A] # interface fc6 enable
[SN5428-2A] # interface fc6 loopback online
```

The following example disables the FC interface *fc3*:

```
[SN5428-2A] # no interface fc3 enable
```


Related Commands	Command	Description
	fcswitch diag	Set all FC interfaces into diagnostic mode for testing purposes.
	fcswitch enable	Enable all FC interfaces.
	interface fc? diag	Set the named FC interface into diagnostic mode for testing purposes.
	interface fc? loopback	Initiate a loopback test on the named FC interface.
	interface fc? reset	Disable and then enable the specified FC interface.
	show fcswitch	Display global configuration information for storage router FC interfaces.

interface fc? ext-credit

To configure the specified interface for credit extension, use the **interface fc? ext-credit** command.

interface fc? ext-credit nn

Syntax Description	<i>fc?</i>	The name of the interface to receive the additional buffer credits. Valid values are fc1 through fc8. When you type the interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
	<i>nn</i>	The maximum number of additional buffer credits available to this interface. Valid values are 0, 11, 22, 33, 44, 55, 66 or 77.

Defaults	No extended credits are available. By default, each FC interface has 12 data buffer credits available.
-----------------	--

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	<p>By default, each SN 5428-2 Storage Router Fibre Channel (FC) interface has a data buffer capacity of 12 maximum sized FC frames or “credits.” This enables full bandwidth class 2 service over a distance of 20 kilometers at 1 Gbps, or 10 kilometers at 2 Gbps, for fibre optic cables. Longer distances can be spanned at full bandwidth by extending the credits available to an interface. An interface configured for credit extension draws on a pool of credits donated by designated donor interfaces. Each donor interface contributes 11 credits to the pool from which the recipient interfaces can draw.</p> <p>In order to receive donated credits, the interface must have a running port type of E_Port, F_Port or G_Port. An interface with a running loop mode port type (FL_Port, GL_Port or translated loop) cannot receive donated credits. In order to donate credits, the interface port type must be <i>donor</i>.</p> <p>Each interface with a port type of <i>donor</i> donates 11 buffer credits; all 11 buffer credits must go to a single recipient interface.</p> <p>Use the show interface command to display the maximum data buffer credits available to an interface, and to display the ports receiving donated credits.</p> <p>To make the interface unavailable for donated data buffer credits, use this command with a maximum number of additional buffer credits of 0 (zero).</p>
-------------------------	--

Examples

The following example sets the port type for interface *fc1* to *F_Port*, sets the port type for interface *fc8* as *donor* (making 11 extended credits available to the interface *fc1*), and configures interface *fc1* for credit extension:

```
[SN5428-2A]# interface fc8 type donor
*[SN5428-2A]# interface fc1 type f-port
*[SN5428-2A]# interface fc1 ext-credit 11
```

The following example makes the interface *fc1* unavailable for credit extension:

```
[SN5428-2A]# interface fc1 ext-credit 0
```

Related Commands

Command	Description
fcswitch interop-credit	Set the data buffer credit capacity for all FC ports.
interface fc? type	Set the port type for the named FC interface.
show fcswitch	Display global configuration information for storage router FC interfaces.
show interface	Display operational and configuration information for the specified interface or all interfaces.

interface fc? fan-enable

To enable Fabric Address Notification (FAN) on the named Fibre Channel (FC) interface, use the **interface fc? fan-enable** command. To disable FAN on the named FC interface, use the **no** form of this command.

interface fc? fan-enable enable

no interface fc? fan-enable enable

Syntax Description	<i>fc?</i>	The name of the FC interface for which you are setting this parameter. Valid values are fc1 through fc8. When you type the interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
	enable	Keyword, required to enable FAN on the named FC interface.

Defaults FAN is enabled on all FC interfaces by default

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use this command to enable or disable FAN loop login behavior on the named FC interface.


Note

All storage routers in a cluster should be configured with the same interface-specific parameters, allowing failover of SCSI routing instances to provide consistent performance characteristics.

Examples The following example disables FAN on the FC interface named *fc6*:

```
[SN5428-2A]# no interface fc6 fan-enable enable
```

The following example enables FAN on the FC interface named *fc3*.

```
[SN5428-2A]# interface fc3 fan-enable enable
```


Related Commands	Command	Description
	interface fc? al-fairness	Enable the fairness algorithm on the named FC interface.
	interface fc? default	Return the named FC interface to its default operational characteristics.
	interface fc? linkspeed	Set the transfer rate for the named FC interface.
	interface fc? mfs-bundle	Enable Multi-Frame Sequence bundling for the named FC interface.
	interface fc? ms-enable	Enable GS-3 management server commands for the specified FC interface.
	interface fc? type	Set the port type for the named FC interface.
	show interface	Display operational and configuration information for the specified interface or all interfaces.

interface fc? linkspeed

To set the transfer rate for the named Fibre Channel (FC) interface, use the **interface fc? linkspeed** command.

```
interface fc? linkspeed {auto | 1gb | 2gb}
```

Syntax Description

fc?	The name of the FC interface for which you are setting this parameter. Valid values are fc1 through fc8. When you type the interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
auto	Keyword, indicating the transfer rate will be negotiated.
1gb	Keyword, indicating the transfer rate will be fixed at 1 Gbps.
2gb	Keyword, indicating the transfer rate will be fixed at 2 Gbps.

Defaults

The transfer rate is automatically negotiated to either 1 Gbps or 2 Gbps, by default.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to change the transfer rate for the named FC interface.


Note

All storage routers in a cluster should be configured with the same interface-specific parameters, allowing failover of SCSI routing instances to provide consistent performance characteristics.

Examples

The following example sets the transfer rate for to 2 Gbps for the FC interface named *fc6*:

```
[SN5428-2A] # interface fc6 linkspeed 2gb
```


Related Commands	Command	Description
	interface fc? al-fairness	Enable the fairness algorithm on the named FC interface.
	interface fc? default	Return the named FC interface to its default operational characteristics.
	interface fc? fan-enable	Enable Fabric Address Notification (FAN) on the named FC interface.
	interface fc? mfs-bundle	Enable Multi-Frame Sequence bundling for the named FC interface.
	interface fc? ms-enable	Enable GS-3 management server commands for the specified FC interface.
	interface fc? type	Set the port type for the named FC interface.
	show interface	Display operational and configuration information for the specified interface or all interfaces.

interface fc? loopback

To initiate a loopback test on the named Fibre Channel (FC) interface, use the **interface fc? loopback** command.

interface fc? loopback {external | internal | online}

Syntax Description	<i>fc?</i>	The name of the FC interface to be tested. Valid values are fc1 through fc8. When you type the interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
	external	Keyword, indicating an external loopback test will be performed. The FC interface must be in a diagnostic state.
	internal	Keyword, indicating an internal loopback test will be performed. The FC interface must be in a diagnostic state.
	online	Keyword, indicating an online loopback test will be performed. The FC interface must be enabled.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Loopback tests are part of standard diagnostic procedures. To display the results or status of a loopback test, use the **show interface fc?** command.

Before performing a loopback test, the named FC interface must be in the correct state.

- For online loopback testing, the FC interface must be enabled. Use the **interface fc? enable** command to enable the FC interface before performing online loopback testing.
- For external or internal loopback testing, the FC interface must be in a diagnostic state. Use the **interface fc? diag** command to set the FC interface into a diagnostic state before performing external or internal loopback testing.

Examples The following example sets the FC interface *fc6* into a diagnostic state and then performs an internal loopback test:

```
[SN5428-2A] # interface fc6 diag
[SN5428-2A] # interface fc6 loopback internal
```


The following example enables the FC interface *fc3* and then performs an online loopback test:

```
[SN5428-2A] # interface fc3 enable
[SN5428-2A] # interface fc3 loopback online
```

Related Commands

Command	Description
fcswitch diag	Set all FC interfaces into diagnostic mode for testing purposes.
fcswitch enable	Enable all FC interfaces.
interface fc? diag	Set the named FC interface into diagnostic mode for testing purposes.
interface fc? enable	Enable the named FC interface.
interface fc? reset	Disable and then enable the specified FC interface.
show interface	Display operational and configuration information for the specified interface or all interfaces.

interface fc? mfs-bundle

To enable Multi-Frame Sequence (MFS) bundling for the named Fibre Channel (FC) interface, use the **interface fc? mfs-bundle** command. To disable MFS bundling for the named FC interface, use the **no** form of this command.

interface fc? mfs-bundle enable timeout nn

no interface fc? mfs-bundle enable


Syntax Description	<i>fc?</i>	The name of the FC interface for which you are setting this parameter. Valid values are fc1 through fc8. When you type the interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
	enable	Keyword, required to enable MFS bundling on the named FC interface.
	timeout nn	The timeout threshold, in milliseconds. Valid values are 10 through 20480. The default timeout value is 10 msec.

Defaults	MFS bundling is enabled on all FC interfaces, by default. The default timeout value is 10 msec.
----------	---

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	MFS bundling is used to support systems that require frames to be sequenced in a particular order.
------------------	--


Note

All storage routers in a cluster should be configured with the same interface-specific parameters, allowing failover of SCSI routing instances to provide consistent performance characteristics.

Examples

The following example enables MFS bundling for the FC interface named *fc6*, and sets the timeout value to 640 msec:

```
[SN5428-2A] # interface fc6 mfs-bundle enable timeout 640
```

The following example disables MFS bundling for the FC interface named *fc3*:

```
[SN5428-2A] # no interface fc3 mfs-bundle enable
```


Related Commands	Command	Description
	interface fc? al-fairness	Enable the fairness algorithm on the named FC interface.
	interface fc? default	Return the named FC interface to its default operational characteristics.
	interface fc? fan-enable	Enable Fabric Address Notification (FAN) on the named FC interface.
	interface fc? linkspeed	Set the transfer rate for the named FC interface.
	interface fc? ms-enable	Enable GS-3 management server commands for the specified FC interface.
	interface fc? type	Set the port type for the named FC interface.
	show interface	Display operational and configuration information for the specified interface or all interfaces.

interface fc? ms-enable

To enable GS-3 management server commands for the specified Fibre Channel (FC) interface, use the **interface fc? ms-enable** command. To disable GS-3 management server commands, use the **no** form of this command.

interface fc? ms-enable enable

no interface fc? ms-enable enable

Syntax Description

<i>fc?</i>	The name of the FC interface for which you are setting this parameter. Valid values are fc1 through fc8. When you type the interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
enable	Keyword, required to enable GS-3 management server commands for the named FC interface.

Defaults

GS-3 management server commands are enabled on all FC interfaces.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Enabling GS-3 management server commands for the FC interface allows in-band management of the SN 5428-2 Storage Router integrated FC switch component. GS-3 management server commands must be enabled if you want to use storage management tools to provide in-band management of the integrated FC switch component along with other switches in the fabric.

Use the **no** form of this command to disable in-band management on the specified FC interface.

Examples

The following example disables GS-3 management server commands for *fc8*:

```
[SN5428-2A] # no interface fc8 ms-enable enable
```

Related Commands

Command	Description
interface fc? default	Return the named FC interface to its default operational characteristics.
show fcswitch	Display global configuration information for storage router 2 FC interfaces.
show interface	Display operational and configuration information for the specified interface or all interfaces.

interface fc? reset

To disable and then enable the specified Fibre Channel (FC) interface, use the **interface fc? reset** command.

interface *fc?* reset

Syntax Description	<i>fc?</i>	The name of the FC interface for which you are setting this parameter. Valid values are fc1 through fc8. When you type the interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
Defaults	None.	
Command Modes	Administrator.	
Command History	Release	Modification
	3.2.1	This command was introduced.
Usage Guidelines	<p>This command is functionally equivalent to issuing a no interface fc? enable command, followed by an interface fc? enable command.</p> <p>After placing the FC interface into diagnostic mode and performing internal loopback testing, use this command to return the interface to an operational state.</p>	
Examples	<p>The following example resets the FC interface named <i>fc3</i>:</p> <pre>[SN5428-2A] # interface fc3 reset</pre>	
Related Commands	Command	Description
	interface fc? diag	Set the named FC interface into diagnostic mode for testing purposes.
	interface fc? enable	Enable the named FC interface.
	interface fc? loopback	Initiate a loopback test on the named FC interface.

interface fc? rscn

To enable the generation of Registered State Control Notification (RSCN) messages on the specified Fibre Channel (FC) interface, use the **interface fc? rscn** command. To disable RSCN messages, use the **no** form of this command.

interface fc? rscn enable

no interface fc? rscn enable

Syntax Description	<i>fc?</i>	The name of the FC interface for which you are setting this parameter. Valid values are fc1 through fc8. When you type the interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
	enable	Keyword, required to enable generation of RSCN messages on the specified interface.

Defaults RSCN messages are generated on all FC interfaces.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Each SN 5428-2 Storage Router and FC switch contains its own local Name Server, called a distributed Name Server (dNS). By default, all SN 5428-2 Storage Routers and FC switches in the fabric distribute RSCN messages whenever a change takes place in their local dNS database. RSCN notification is used to maintain the integrity of the local dNS database.

Examples The following example disables generation of RSCN messages on interface *fc5*:

```
[SN5428-2A] # no interface fc5 rscn enable
```

Related Commands	Command	Description
	show fcswitch nameserver	Display the local Fibre Channel nameserver database.

interface fc? type

To set the port type for the named Fibre Channel interface, use the **interface fc? type** command.

```
interface fc? type {auto | f-port | fl-port | g-port | gl-port}
```

```
interface fc? type tl-port mode {autobridge | autolearn}
```

```
interface fc? type donor
```

Syntax Description		
	<i>fc?</i>	The name of the FC interface for which you are setting this parameter. Valid values are fc1 through fc8. When you type the interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
	auto	Keyword, indicating the port type is automatically negotiated and functions as a generic loop (GL_Port).
	f-port	Keyword, indicating the port type is fabric. F_Ports are fabric ports.
	fl-port	Keyword, indicating the port type is fabric loop (also known as “public loop”).
	g-port	Keyword, indicating the port type is generic and can function as either an F_Port or an E_Port. An E_Port (also known as an “expansion port”) is used to link multiple FC switches together into a fabric.
	gl-port	Keyword, indicating the port type is generic loop and can function as either an F_Port, an FL_Port or an E_Port.
	tl-port	Keyword, indicating the port type is translated loop.
	mode autobridge	Keywords, indicating public targets are made visible to the initiator in a private loop.
	mode autolearn	Keywords, indicating targets in a private loop are made visible.
	donor	Keyword, indicating the interface is functioning as a donor port, making 11 buffer credits available to a recipient port, configured for credit extension.

Defaults The port type is *generic loop* (GL_Port), by default.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Select the appropriate port type based on the connected equipment. By default, all of the storage router FC ports are defined as self configuring GL_Ports.

- A GL_Port configures as an FL_Port when connected to a loop of public devices, an F_Port when connected to a single device, or an E_Port when connected to another SN 5428-2 or an FC-SW-2 compliant switch. A GL_Port may also configure as an E_Port when connected to a switch running non-FC-SW-2 compliant firmware.
- A G_Port configures as an F_Port when connected to a single public device or an E_Port when connected to another SN 5428-2 or an FC-SW-2 compliant switch. A G_Port may also configure as an E_Port when connected to a switch running non-FC-SW-2 compliant firmware.
- An F_Port supports connection to a single public device (N_Port).
- An FL_Port supports connection to a loop of up to 126 public devices (NL_Port).
- A TL_Port supports connection to a loop of up to 126 private devices with the ability to communicate with “off-loop” devices, such as public fabric devices and private devices on other TL_Ports. TL_Ports connect to devices that confirm to the Fibre Channel-Private Loop SCSI Direct Attach (FC-PLDA) standard. A TL_Port acts as a proxy for the off-loop device, translating private frames to and from public frames. Each TL_Port can proxy up to 64 off-loop devices.
- A donor port type indicates that the interface is donating its buffer credits and is not used for FC devices. Each donor ports donates 11 buffer credits to the pool. All of the 11 credits must go to a single recipient interface, configured for credit extension.

Public devices have full Fibre Channel addressing capability and can communicate with any other public device on the fabric; private devices do not have full FC addressing capability. Private devices have only the Arbitrated Loop Physical Address (ALPA) portion.

**Note**

All storage routers in a cluster should be configured with the same interface-specific parameters, allowing failover of SCSI routing instances to provide consistent performance characteristics.

Examples

The following example sets the port type to fabric for the FC interface named *fc6*:

```
[SN5428-2A] # interface fc6 type f-port
```

The following example set the port type to translated loop for the FC interface named *fc3*. The mode is *autolearn*, so targets in private loop are made visible.

```
[SN5428-2A] # interface fc3 type tl-port mode autolearn
```

The following example sets the port type for interface *fc1* to *F_Port*, sets the port type for interface *fc8* as *donor* (making 11 buffer credits available to the interface *fc1*), and configures interface *fc1* for credit extension:

```
[SN5428-2A] # interface fc1 type f-port
* [SN5428-2A] # interface fc8 type donor
* [SN5428-2A] # interface fc1 ext-credit 11
```


Related Commands	Command	Description
	interface fc? al-fairness	Enable the fairness algorithm on the named FC interface.
	interface fc? default	Return the named FC interface to its default operational characteristics.
	interface fc? ext-credit	Configure the specified interface as a potential recipient of donated data buffer credits.
	interface fc? fan-enable	Enable Fabric Address Notification (FAN) on the named FC interface.
	interface fc? linkspeed	Set the transfer rate for the named FC interface.
	interface fc? mfs-bundle	Enable Multi-Frame Sequence bundling for the named FC interface.
	interface fc? ms-enable	Enable GS-3 management server commands for the specified FC interface.
	show interface	Display operational and configuration information for the specified interface or all interfaces.

interface fci? devicediscoverytimer

To enable the SN 5428-2 Storage Router internal Fibre Channel (FC) interfaces to perform background device rediscovery for all attached FC targets at specific time intervals, use the **interface fci? devicediscoverytimer** command.

interface fci? devicediscoverytimer nn

Syntax Description	<i>fci?</i>	The name of the internal FC interface. Valid values are fci1 or fci2. When you type the interface fci? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
	<i>nn</i>	The amount of time, in minutes between automatic background device rediscovery.

Defaults	The device discovery timer value is 0, indicating that automatic background device rediscovery is disabled.
-----------------	---

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modifications
	3.2.1	This command was introduced.

Usage Guidelines	<p>Use this command to enable automatic device rediscovery on a periodic basis in environments where LUNs can be created on FC targets, but no event occurs to cause devices to be rediscovered. This situation may occur with certain RAID controllers or virtualization type devices.</p> <p>You do not need to issue the interface fci? devicediscoverytimer command for both internal FC interfaces. When you enable automatic background device rediscovery for one internal FC interface (for example, fci1), the same setting is enabled for the other internal FC interface (for example, fci2).</p> <p>When automatic background device rediscovery is enabled, use the show interface command with the stats keyword to display the current device rediscovery timer configuration.</p>
-------------------------	--

Examples	<p>The following example enables automatic device rediscovery every 20 minutes:</p> <pre>[SN5428-2A]# interface fci2 devicediscoverytimer 20 device discovery timer changed to 20 minutes on interface fci1 device discovery timer changed to 20 minutes on interface fci2</pre> <p>The following example disables automatic background device rediscovery by setting the device discovery timer interval to 0. (This is the default setting.)</p> <pre>[SN5428-2A]# interface fci2 devicediscoverytimer 0 device discovery timer changed to 0 minutes on interface fci1 device discovery timer changed to 0 minutes on interface fci2</pre>
-----------------	--

Use the show interface command with the stats keyword to display the current device rediscovery timer configuration. In the following example, the storage router will perform background device rediscovery every 10 minutes.

```
[SN5428-2B]# show interface fci1 stats
loop:          LOOP READY
connection:    F Port
Data Rate:     2 Gb/s
port id:       0x20f00
ALPA:          0x0
firmware:      READY
device rediscovery timer: 10 minutes
. . .
```

**Note**

The device rediscovery timer information does not display if automatic background device rediscovery is not enabled.

Related Commands

Command	Description
show interface	Display operational and configuration information for the specified interface or all interfaces.

interface ge?

To set various operational parameters associated with the Gigabit Ethernet interface, such as the size of the maximum transfer unit (MTU) or the use of VLANs, use the **interface ge?** command. To disable the use of VLANs, use the **no** form of this command. To specify that auto negotiation will never be used on this interface, use the **interface ge? no autonegotiation** command.

interface ge? {autonegotiation [autodetect] | mtusize {nn | default}}

interface ge? no autonegotiation

interface ge? vlan enable

no interface ge? vlan enable

Syntax Description

<i>ge?</i>	The name of the interface for which you are setting this parameter. When you type the interface ge? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
autonegotiation	Auto negotiation will always be used on this interface.
autonegotiation autodetect	Automatically detect if auto negotiation should be used for this interface. This is the default setting.
mtusize nn	The size of the MTU, in bytes. <i>nn</i> is an integer between 1500 and 9000 inclusive.
mtusize default	Reset the value to the factory default of 1500 bytes.
vlan enable	Enable VLANs for this interface. This is the default.

Defaults

MTU size defaults to 1500 bytes. Auto negotiation defaults to *autodetect*. For storage routers deployed for SCSI routing, the use of VLANs is enabled by default.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

All storage routers in a cluster should be configured with the same MTU size and other interface-specific parameters, allowing failover of applications to provide consistent performance characteristics.

If the SN 5428-2 is deployed for FCIP, a larger MTU size is desirable. Set the MTU size to 9000 bytes, if possible.

Use the **no interface ge? vlan enable** command to quickly restrict VLAN functionality on the Gigabit Ethernet interface for troubleshooting purposes.

Examples

The following example enables auto negotiation on the Gigabit Ethernet interface, *ge1*. The *ge1* interface will not come up until auto negotiation is successfully completed.

```
[SN5428-2A] # interface ge1 autonegotiation
```

The following example disables VLANs for the Gigabit Ethernet interface, *ge2*:

```
[SN5428-2A] # no interface ge2 vlan enable
```

The following examples changes the MTU size for the Gigabit Ethernet interface, *ge1*, to 9000 bytes. This is the recommended setting when the storage router is deployed for FCIP.

```
[SN5428-2A] # no interface ge2 vlan enable
```

Related Commands

Command	Description
show interface	Display operational and configuration information for the specified interface or all interfaces.

interface ge? ip-address

To enable an IP address on a Gigabit Ethernet interface for management of the SN 5428-2 Storage Router, use the **interface ge? ip-address** command. To disable an IP address configured for storage router management, use the **no** form of this command.

interface ge? [vlan vid] ip-address {A.B.C.D/bits | A.B.C.D/1.2.3.4} [secondary ge?]

no interface ge? [vlan vid] ip-address

Syntax Description	<i>ge?</i>	The name of the Gigabit Ethernet interface associated with this IP address. When you type the interface ge? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
	vlan <i>vid</i>	The keyword and the VLAN identifier.
	<i>A.B.C.D/bits</i>	The IP address of the specified Gigabit Ethernet interface to be used for management of the SN 5428-2 Storage Router. If the keyword vlan is used, the IP address is part of the specified VLAN. The <i>/bits</i> specifies the network mask in CIDR style.
	<i>A.B.C.D/1.2.3.4</i>	The IP address of the specified Gigabit Ethernet interface to be used for management of the SN 5428-2 Storage Router. If the keyword vlan is used, the IP address is part of the specified VLAN. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask.
	secondary <i>ge?</i>	(Optional) The name of the Gigabit Ethernet interface to be used as a secondary interface for the specified IP address. If the primary interface goes down and remains down for two seconds, the specified IP address will be moved to the secondary interface.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use this command to designate an IP address on a Gigabit Ethernet interface to be used for management of the SN 5428-2 Storage Router (in-band management). The Gigabit Ethernet IP address specified for storage router management can perform all the normal management tasks, but unlike the management interface, it cannot perform HA functions in a cluster environment if the HA interface is unavailable.

In-band management is performed via a Telnet or Secure Shell (SSH) session, or via the web-based GUI. Only one IP address per logical interface can be configured for in-band management. Telnet, SSH, HTTP and SSL access is restricted, by default, on all Gigabit Ethernet interfaces. Use the **no restrict** CLI command to allow access to the storage router using the desired protocol via the specified Gigabit Ethernet interface.

If the **secondary** keyword is used, both Gigabit Ethernet interfaces must be connected to the same network segment. If you configure a Gigabit Ethernet IP address with a secondary interface, all Gigabit Ethernet IP addresses on the same subnet must also be configured with the same secondary interface.

If you are using the Gigabit Ethernet interface IP address in configuration of external servers, such as RADIUS, TACACS+ or SNMP, that will access the storage router via this interface, reboot the storage router after configuring the Gigabit Ethernet IP address and saving the change to the system bootable configuration. This assures that the IP address is the first address associated with the specified interface.

**Note**

The IP address used for management of the SN 5428-2 Storage Router cannot be used as a Gigabit Ethernet IP address associated with a SCSI routing instance (serverif); the IP address must not already be in use on the storage router.

Examples

The following example configures the IP address *10.1.0.244/24* on *ge1* for management of the storage router, and enables the *ge1* interface for Telnet access.

```
[SN5428-2B] # interface ge1 ip-address 10.1.0.244/24
[SN5428-2B] # no restrict ge1 telnet
```

The following example configures two IP addresses on unique logical interfaces for storage router management. The IP address *10.1.0.160/255.255.255.128* is specified as part of VLAN *100* on *ge2*; the IP address *10.1.0.168/255.255.255.128* is also on *ge2* but is not part of a VLAN. The interface *ge2* is enabled for SSH access.

```
[SN5428-2B] # interface ge2 vlan 100 ip-address 10.1.0.160/255.255.255.128
[SN5428-2B] # interface ge2 ip-address 10.1.0.168/255.255.255.128
[SN5428-2B] # no restrict ge2 ssh
```

The following example configures the IP address *10.1.0.230/24* on *ge2* for storage router management. If the *ge2* interface is unavailable, the *ge1* interface will be used. Both *ge1* and *ge2* are enabled for HTTP access.

```
[SN5428-2B] # interface ge2 ip-address 10.1.0.230/24 secondary ge1
[SN5428-2B] # no restrict ge2 http
[SN5428-2B] # no restrict ge1 http
```

The following example removes the IP address configured for storage router management from *ge1*, and restricts SSL access to the interface:

```
[SN5428-2B] # no interface ge1 ip-address
[SN5428-2B] # restrict ge1 ssl
```

The following example configures the IP address *10.1.0.212/24* on *ge2* for management of the storage router, saves the changes to the bootable configuration, and then performs a fast reboot. This assures that the IP address will be the first address associated with the *ge2* interface, and allows the IP address to be used by external servers (such as RADIUS or TACACS+) to communicate with the storage router.

```
[SN5428-2B] # interface ge2 ip-address 10.1.0.212/24
*[SN5428-2B] # save all bootconfig
[SN5428-2B] # reboot fast
```


Related Commands	Command	Description
	restrict	Secure access to storage router interfaces by communications protocols and services.
	show interface	Display operational and configuration information for the specified interface or all interfaces.
	show ip	Display entries from the SN 5428-2 Storage Router routing table and statistics about the protocols used in the SN 5428-2 network.
	show restrict	Display configurable security settings for the storage router interfaces.

interface ha

To set various operational parameters associated with the high availability (HA) interface, such as the speed and duplex mode, use the **interface ha** command.

interface ha autonegotiation

interface ha no autonegotiation [speed {10 | 100}] [duplex {full | half}]

Syntax Description	autonegotiation	Auto negotiation will always be used on this interface. Operational characteristics will automatically be negotiated with the partner.
	speed 10	(Optional) The interface speed is fixed at 10 Mbps. Auto negotiation is not used.
	speed 100	(Optional) The interface speed is fixed at 100 Mbps. Auto negotiation is not used. If speed is not specified, the default is 100 Mbps.
	duplex full	(Optional) The duplex setting is fixed at full. Auto negotiation is not used. If the duplex setting is not specified, the default is full duplex.
	duplex half	(Optional) The duplex setting is fixed at half. Auto negotiation is not used.

Defaults	Auto negotiation is enabled.
----------	------------------------------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to manually set a specific interface speed and duplex setting, if the partner is unable to auto negotiate these settings.
------------------	--

All storage routers in a cluster should be configured with the same interface-specific parameters, allowing failover to provide consistent performance characteristics. Use the **show interface ha** command to display current operating characteristics for the HA interface.

Examples	The following example disables auto negotiation, and sets the interface speed to 10 Mbps, duplex full:
----------	--

[SN5428-2A] **interface ha no autonegotiation speed 10 duplex full**

Related Commands	Command	Description
	interface ha ip-address	Specify the HA interface IP address and subnet mask.
	show interface	Display operational and configuration information for the specified interface or all interfaces.

interface ha ip-address

To specify the IP address and subnet mask for this system's high availability interface, use the **interface ha ip-address** command.

interface ha ip-address {*A.B.C.D/bits* | *A.B.C.D/1.2.3.4*}

Syntax Description

<i>A.B.C.D/nn</i>	The IP address of the HA interface. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style.
<i>A.B.C.D/1.2.3.4</i>	The IP address of the HA interface. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The HA features are used within a cluster of storage routers. Each member of the cluster communicates over the HA and management interfaces, exchanging heartbeats and other configuration information, allowing for failover in case of system problems.

The HA interface and the management interface must be on unique IP subnets. In a cluster, the HA interfaces for all nodes should be on the same IP subnet.

After initial system configuration, use the **setup cluster** command to change the configuration of the high availability environment.

For SN 5428-2 Storage Routers deployed for transparent SCSI routing, or standalone storage routers deployed for SCSI routing, the HA interface is optional.

Examples

The following example assigns the IP address of 10.1.20.56/24 to the HA interface:

```
[SN5428-2B] # interface ha ip-address 10.1.20.56/24
```


Related Commands	Command	Description
	interface mgmt ip-address	Specify the management interface IP address and subnet mask.
	save all	Save all configuration information.
	save system	Save selected system configuration information, including HA IP address.
	setup cluster	Change the configuration of the high availability environment.
	show cluster	Display cluster-related operational statistics, including heartbeat information.
	show ha	Display HA operational statistics for the storage router or for a specific application.

interface mgmt

To set various operational parameters associated with the management interface, such as the speed and duplex mode, use the **interface mgmt** command.

interface mgmt autonegotiation

interface mgmt no autonegotiation [speed {10 | 100}] [duplex {full | half}]

Syntax Description	autonegotiation	Auto negotiation will always be used on this interface. Operational characteristics will automatically be negotiated with the partner.
	speed 10	(Optional) The interface speed is fixed at 10 Mbps. Auto negotiation is not used.
	speed 100	(Optional) The interface speed is fixed at 100 Mbps. Auto negotiation is not used. If speed is not specified, the default is 100 Mbps.
	duplex full	(Optional) The duplex setting is fixed at full. Auto negotiation is not used. If the duplex setting is not specified, the default is full duplex.
	duplex half	(Optional) The duplex setting is fixed at half. Auto negotiation is not used.

Defaults	Auto negotiation is enabled.
----------	------------------------------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to manually set a specific interface speed and duplex setting, if the partner is unable to auto negotiate these settings.
------------------	--

All storage routers in a cluster should be configured with the same interface-specific parameters, allowing failover to provide consistent performance characteristics. Use the **show interface mgmt** command to display current operating characteristics for the management interface.

Examples	The following example disables auto negotiation, and sets the interface speed to 10 Mbps, duplex full: [SN5428-2A] interface mgmt no autonegotiation speed 10 duplex full
----------	---

Related Commands	Command	Description
	interface mgmt ip-address	Specify the management interface IP address and subnet mask.
	show interface	Display operational and configuration information for the specified interface or all interfaces.

interface mgmt ip-address

To specify the IP address and subnet mask of the interface labeled MGMT on the front panel of the SN 5428-2 Storage Router, use the **interface mgmt ip-address** command. This address is used to manage the storage router via Telnet, Secure Shell (SSH), the web-based GUI, or SNMP.

interface mgmt ip-address {*A.B.C.D/bits* | *A.B.C.D/1.2.3.4*}

Syntax Description	<i>A.B.C.D/bits</i>	The IP address of the management interface. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style.
	<i>A.B.C.D/1.2.3.4</i>	The IP address of the management interface. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask.

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	The management and HA interfaces must be on unique IP subnets. In a cluster, the management interfaces for all nodes should be on the same IP subnet.
------------------	---

Examples	<p>The following example assigns the IP address of <i>10.1.10.244/24</i> to the management interface:</p> <pre>[SN5428-2A]# interface mgmt ip-address 10.1.10.244/24</pre>
----------	---

Related Commands	Command	Description
	interface ha ip-address	Specify the HA interface IP address and subnet mask.
	ip route	Add a static route to the SN 5428-2 Storage Router routing table.
	save all	Save all configuration information.
	save system	Save selected system configuration information, including management and HA interface information.
	setup mgmt	Run the wizard to configure the management interface.
	show cluster	Display cluster-related operational statistics, including heartbeat information.
	show interface	Display operational and configuration information for the specified interface or all interfaces.

ip default-gateway

To add a gateway to the default route in the SN 5428-2 Storage Router routing table, use the **ip default-gateway** command. To delete the gateway, use the **no** form of this command.

ip default-gateway *E.F.G.H* [*administrative-distance*]

no ip default-gateway [*A.B.C.D*]

Syntax Description	<i>E.F.G.H</i>	The default gateway IP address.
	<i>administrative-distance</i>	(Optional) The administrative distance for the route. Valid values are 0 to 255 inclusive. The default administrative distance is 1.
	<i>A.B.C.D</i>	(Optional) The IP address of the default route. The gateway to this route will be removed.

Defaults	The default administrative distance for a static route is 1.
----------	--

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	<p>All IP interfaces in the SN 5428-2 use the routing table to reach services and networks outside their local network. Other facilities, such as SNMP and connections to an NTP server or DNS servers, may also use the routing table. Use the ip default-gateway command to add a gateway to the default route in this table.</p>
------------------	--

Only one default route is allowed in the routing table.



Note	This command is functionally equivalent to issuing the ip route command for IP address 0.0.0.0/00.
------	---

The administrative distance is used to determine which route to install in the routing table when there are multiple routes to the same destination. The default administrative distance for static routes is 1; the administrative distance for dynamic routes created by RIP is 120. The route with the lower administrative distance is installed in the routing table (as long as the interface used by the route is up).

By default, a static route will always override a dynamic route learned by RIP. To modify this behavior, change the administrative distance of a static route to a value greater than 120.

Examples	The following example adds a default route to gateway <i>10.3.40.1</i> in the routing table. The administrative distance is 1, by default.
----------	--

```
[SN5428-2A] # ip default-gateway 10.3.40.1
```


The following example adds a default route to gateway *10.3.30.1*, with an administrative distance of *130*, in the routing table. If RIP is enabled for the storage router, the default route can be overridden by a dynamically learned route.

```
[SN5428-2A] # ip default-gateway 10.3.30.1 130
```

Related Commands	Command	Description
	ip route	Add a static route to the SN 5428-2 Storage Router routing table.
	show ip	Display entries from the SN 5428-2 Storage Router routing table and statistics about the protocols used in the storage router network.
	show route	Display the default routes.

ip domain-name

To specify the name of the SN 5428-2 Storage Router domain, use the **ip domain-name** command. To remove a domain name, use the **no** form of this command.

ip domain-name *name*

no ip domain-name

Syntax Description	<i>name</i>	The name of the SN 5428-2 Storage Router domain.
--------------------	-------------	--

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use the ip domain-name command in conjunction with the ip name-server command. The storage router requires access to a DNS if any IP addresses are entered as host names via any of the storage router management interfaces, or if the management interface IP address is to be correlated with a DNS host name.
------------------	---



Note

If the DNS is outside the storage router management subnet, use the **ip route** command to add an appropriate gateway IP address to the routing table.

Examples	The following example assigns the domain name <i>abc123z.com</i> to the storage router.
----------	---

```
[SN5428-2A] # ip domain-name abc123z.com
```

Related Commands	Command	Description
	ip default-gateway	Configure a gateway for the default route.
	ip name-server	Specify the IP addresses of a primary (and optional secondary) DNS.
	ip route	Add a static route to the SN 5428-2 Storage Router routing table.
	setup mgmt	Run the wizard to configure the management interface.

ip name-server

To specify the IP address of the primary and optional secondary Domain Name Server (DNS), use the **ip name-server** command. To remove the settings for current domain name servers, use the **no** form of this command.

ip name-server *A.B.C.D* [*E.F.G.H*]

no ip name-server

Syntax Description	<i>A.B.C.D</i>	The IP address of a primary Domain Name Server, accessible by the storage router. <i>A.B.C.D</i> is the dotted quad notation of the IP address.
	<i>E.F.G.H</i>	(Optional) The IP address of a secondary DNS, accessible by the storage router. <i>E.F.G.H</i> is the dotted quad notation of the IP address.

Defaults None.

Command Modes Administrator.

Command History	Release	Configuration
	3.2.1	This command was introduced.

Usage Guidelines The storage router requires access to a DNS if any IP addresses are entered as host names via any of the storage router management interfaces, or if the management interface IP address is to be correlated with a DNS host name. To use the services of a DNS, you must also assign a domain name to the storage router via the **ip domain-name** command.

If the DNS is outside the storage router management subnet, use the **ip route** command to add an appropriate gateway IP address to the routing table.

Examples The following example assigns the domain name *abc123z.com* to the storage router, and assigns the IP address of the primary DNS to *10.1.40.243* and the secondary DNS to *10.1.50.249*:

```
[SN5428-2A] # ip domain-name abc123z.com
[SN5428-2A] # ip name-server 10.1.40.243 10.1.50.249
```

Related Commands	Command	Description
	ip default-gateway	Configure a gateway for the default route.
	ip domain-name	Assign a domain name to the SN 5428-2 Storage Router.
	ip route	Add a static route to the SN 5428-2 Storage Router routing table.
	setup mgmt	Run the wizard to configure the management interface.

ip radius sourceinterface

To specify a single network interface to be used as the source IP address for all outgoing AAA authentication requests to RADIUS servers, use the **ip radius sourceinterface** command. To disable this restriction, use the **no** form of this command.

ip radius sourceinterface *if-name*

no ip radius sourceinterface

Syntax Description	<i>if-name</i>	The name of the interface to which you are restricting all outgoing AAA authentication requests to RADIUS servers. When you type the IP radius sourceinterface ? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
Defaults	None.	
Command Modes	Administrator.	
Command History	Release	Modification
	3.2.1	This command was introduced.
Usage Guidelines	Use this command to restrict all outgoing AAA authentication requests to RADIUS servers to a single interface.	
Examples	<p>The following example restricts all outgoing AAA authentication requests to RADIUS servers to the Gigabit Ethernet interface <i>ge1</i>:</p> <pre>[SN5428-2A] # ip radius sourceinterface ge1</pre>	

Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	show aaa	Display AAA configuration information.

ip rip enable

To enable the SN 5428-2 Storage Router to learn dynamic routing using the routing information protocol (RIP), use the **ip rip enable** command. To disable dynamic routing via RIP, use the **no** form of this command.

ip rip enable

no ip rip enable

Syntax Description

This command has no arguments or keywords.

Defaults

RIP is disabled by default.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Routing Information Protocol (RIP) is an Interior Gateway Protocol (IGP) for dynamic routing and uses a distance vector algorithm to determine the best route between nodes in an Autonomous System (AS).

The SN 5428-2 Storage Router is a passive, or silent, RIP device; it updates routes based on RIP advertisements but it does not advertise. The storage router listens for advertised routes, learning routing information dynamically as it is exchanged in the network. The storage router supports both RIP version 1 (v1) and RIP version 2 (v2).

The SN 5428-2 RIP implementation runs RIP v2 in broadcast mode. This allows the storage router to learn from either RIP v1 or RIP v2 hosts that are operating in broadcast mode. The storage router will not learn routes from RIP v2 hosts operating in multicast mode.

If you are using RIP in your network, you can enable RIP support on the storage router. RIP eliminates or reduces the need to configure static routes for the storage router, because the storage router updates the route table based on the RIP advertisements.

The storage router can learn a maximum of 200 routes. Additional routes that are received are silently ignored. In the routing table, a static route will always override a dynamic route by default. To modify this behavior, change the administrative distance of a static route to a value greater than 120.

Examples

The following example enables RIP for the SN 5428-2 Storage Router:

```
[SN5428-2A]# ip rip enable
[SN5428-2A] Dec 09 17:54:16: %IP-5-IRMRSAR: RIP Services are running
```

The following command disables RIP:

```
[SN5428-2A]# no ip rip enable
```


Related Commands	Command	Description
	ip rip timers	Configure various RIP timers.
	show ip	Display entries from the SN 5428-2 Storage Router routing table, and statistics about the protocols used in the storage router network. Use the rip keyword to display RIP configuration information.

ip rip timers

To configure various RIP timers, use the **ip rip timers** command.

ip rip timers invalid {*nn* | **default**}

Syntax Description	invalid <i>nn</i>	Specifies the maximum time, in seconds, between updates before a route is expired and made a candidate for removal from the routing table.
	default	Keyword, used to return the specified timer to the default value. The default invalid timer is 180 seconds.

Defaults	The RIP invalid timer defaults to 180 seconds.
-----------------	--

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Routing Information Protocol (RIP) is an Interior Gateway Protocol (IGP) for dynamic routing and uses a distance vector algorithm to determine the best route between nodes in an Autonomous System (AS). The SN 5428-2 Storage Router is a passive, or silent, RIP device; it updates routes based on RIP advertisements but it does not advertise. The storage router listens for advertised routes, learning routing information dynamically as it is exchanged in the network. The storage router supports both RIP version 1 (v1) and RIP version 2 (v2).

The SN 5428-2 RIP implementation runs RIP v2 in broadcast mode. This allows the storage router to learn from either RIP v1 or RIP v2 hosts that are operating in broadcast mode. The storage router will not learn routes from RIP v2 hosts operating in multicast mode.

The storage router can learn a maximum of 200 routes. Additional routes that are received are silently ignored. In the routing table, a static route will always override a dynamic route by default. To modify this behavior, change the administrative distance of a static route to a value greater than 120.

Timers are used to configure the timing of RIP activities. The invalid timer configures the maximum amount of time between updates of the internal route table. Use the **default** keyword to return a RIP timer to its default value.

Examples	The following example sets the RIP invalid timer to a value of 200 seconds and saves all configuration changes. This is the maximum amount of time between updates before a route is marked as expired.
-----------------	---

```
[SN5428-2A] # ip rip timers invalid 200
* [SN5428-2A] # save all bootconfig
```


Related Commands	Command	Description
	ip rip enable	Enable the storage router to learn dynamic routing using the routing information protocol (RIP).
	show ip	Display entries from the SN 5428-2 Storage Router routing table, and statistics about the protocols used in the storage router network. Use the rip keyword to display RIP configuration information.

ip route

To add a static route to the SN 5428-2 Storage Router routing table, use the **ip route** command. The specified IP address is accessed via the gateway specified in the command. To remove a static route from the routing table, use the **no** form of this command.

ip route {*A.B.C.D/bits* | *A.B.C.D/1.2.3.4*} *E.F.G.H* [*administrative-distance*]

no ip route {*A.B.C.D/bits* | *A.B.C.D/1.2.3.4*} [*E.F.G.H*]

Syntax Description

<i>A.B.C.D/bits</i>	The IP address of the static route. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style.
<i>A.B.C.D/1.2.3.4</i>	The IP address of the static route. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask.
<i>E.F.G.H</i>	The gateway IP address through which the static route (<i>A.B.C.D/bits</i> or <i>A.B.C.D/1.2.3.4</i>) is accessed.
<i>administrative-distance</i>	(Optional) The administrative distance for the route. Valid values are 0 to 255 inclusive. The default administrative distance is 1.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

All IP interfaces in the storage router use the routing table to reach services and networks outside their local network. Other facilities, such as SNMP and connections to an NTP server or DNS servers, may also use the routing table. Use the **ip route** command to specify routes for servers or networks outside the local networks associated with the storage router IP interfaces.

Use the **show ip route** command to display the SN 5428-2 Storage Router routing table. Use the **show route** command to display all the default routes, included the routes that have been configured but not added to the routing table.

The administrative distance is used to determine which route to install in the routing table when there are multiple routes to the same destination. The default administrative distance for static routes is 1; the administrative distance for dynamic routes created by RIP is 120. The route with the lower administrative distance is installed in the routing table (as long as the interface used by the route is up).

By default, a static route will always override a dynamic route learned by RIP. To modify this behavior, change the administrative distance of a static route to a value greater than 120.

**Note**

A route is not added to the routing table until the associated IP gateway address is configured. The CLI displays an informational message if a route is added for an IP address that is not yet configured.

Examples

The following command adds a unique route for IP address *10.1.30.0*, specifying the subnet mask in dotted quad notation:

```
[SN5428-2A]# ip route 10.1.30.0/255.255.255.0 10.1.10.10
```

The following command adds a unique route for IP address *10.1.40.0*, using gateway *10.1.10.10*, which is not yet on a locally connected network. The message indicates that the route has been configured but has not yet been made operational in the storage router.

```
[SN5428-2A]# ip route 10.1.40.0/24 10.1.10.10
```

```
Oct 25 19:25:17: %UI-4-NMREE01: Gateway 10.1.10.10 used by route 10.1.40.0/24 is currently unreachable
```

The following command adds a unique route for IP address *10.1.20.0* with an administrative distance of *130*, in the routing table. If RIP is enabled for the storage router, the route can be overridden by a dynamically learned route.

```
[SN5428-2A]# ip route 10.1.20.0/24 10.1.10.10 130
```

Related Commands

Command	Description
ip default-gateway	Configure a gateway for the default route.
ip domain-name	Assign a domain name to the SN 5428-2 Storage Router.
ip name-server	Specify the IP addresses of a primary (and optional secondary) DNS.
show ip	Display entries from the SN 5428-2 Storage Router routing table, and statistics about the protocols used in the storage router network.
show route	Display the default routes.

ip tacacs sourceinterface

To specify a single network interface to be used as the source IP address for all outgoing AAA authentication requests to TACACS+ servers, use the **ip tacacs sourceinterface** command. To disable this restriction, use the **no** form of this command.

ip tacacs sourceinterface *if-name*

no ip tacacs sourceinterface

Syntax Description

<i>if-name</i>	The name of the interface to which you are restricting all outgoing AAA authentication requests to TACACS+ servers. When you type the IP tacacs sourceinterface ? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
----------------	---

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to restrict all outgoing AAA authentication requests to TACACS+ servers to a single interface.

Examples

The following example restricts all outgoing AAA authentication requests to TACACS+ servers to the management interface, *mgmt*:

```
[SN5428-2A] # ip tacacs sourceinterface mgmt
```


Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

logging #?

To insert a routing rules entry into the logging table before the specified entry, use the **logging #?** command.

logging #?

logging #nn level notification-level from facility-name to destination1 [destination2...]

Syntax Description	#?	Request an indexed list of entries in the logging table.
	#nn	The index number from the displayed list of entries. The new routing rule will be inserted before the specified logging table entry.
	notification-level	Limit logging to messages of a specified level or lower levels. See Table 12-10 in the Usage Guidelines section for a list of valid names that can be used for the <i>notification-level</i> argument.
	from facility-name	The name of the facility. A facility is the feature area from which the message is received. See Table 12-11 in the Usage Guidelines section for a list of valid facility names. Each facility can have eight notification levels. Each notification level can have up to seven destination.
	to destination1 [destination2...]	At least one of the destinations described in Table 12-12 .

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Event, trace and debug messages can be routed to various destinations, based on the notification level of the message and the application area (facility) that generated the message. When a log message is received by the storage router, the logging table rules are searched by facility name and by message level until a match is found. The log message is sent to all the destinations specified by the matching rule.

New routing rules are normally appended to the existing rules in the table. Use this command to insert a routing rule at a specific location within the table.

To display an indexed lists of entries in the logging table, use the number sign (#) character followed by a question mark (?). That action will cause the routing rules in the logging table to be displayed as a numbered (indexed) set of lines. The command is displayed at the prompt below the list to the point of the # keyword. Complete the command by entering the appropriate index number and the desired keywords and variables to compose the new routing rule. The new routing rule will be added to the table before the specified entry.

The level limits logging to messages of the specified notification level or lower levels, based on level number. [Table 12-10](#) describes the available logging levels.

Table 12-10 Logging Level Notification Levels and Corresponding Numbers

Notification Level	Level Number	Description
emergency	0	System unusable
alert	1	Immediate action needed
critical	2	Critical conditions
error	3	Error conditions
warning	4	Non-fatal warning conditions
notice	5	Normal but significant conditions
info	6	Informational messages only
debug	7	Information for troubleshooting purposes



Note

The debug notification level should be used for specific troubleshooting purposes only. System performance and HA behavior may be adversely affected by logging at the debug notification level.

Each facility can have up to eight notification levels. Each facility and notification level pair can have up to seven destinations. [Table 12-11](#) describes the available facility names.

Table 12-11 Logging Level Facilities

Facility Name	Description
all	All facilities.
AUTH	AAA authentication.
CDP	Cisco Discovery Protocol.
CONF	Configuration functions.
FC	Fibre Channel interfaces.
FCIP	FCIP functions.
GE	Gigabit Ethernet interfaces.
HA	High availability cluster functions.
IF	Interface manager.
INVALID	Generic functions.
IP	IP functions.
ISCSI	iSCSI functions.
MON	Hardware monitor.
SLP	Service Location Protocol service functions.
SNMP	Simple Network Management Protocol.
SYSLOG	Syslog functions.

Table 12-11 Logging Level Facilities (continued)

Facility Name	Description
UI	User interface functions.
VTP	VTP and VLAN functions.

Table 12-12 describes the available logging destinations.

Table 12-12 Logging Level Destinations

Destination	Description
all	Logs to all destinations.
none	No logging occurs.
console	Logs to serial console CLI sessions.
logfile	Logs messages to the storage router log file.
rslog	Logs messages to a remote syslog server. Use the logging syslog command to specify the IP address of the remote syslog server.
vty	Logs to all Telnet, SSH, or other virtual terminal CLI sessions.

Use the **save system bootconfig** or **save all bootconfig** commands to save the list of log route entries. To delete a log route entry by its index number, use the **delete logging** command.

Examples

The following example displays an indexed list of the routing rules in the logging table, and then inserts an entry to log anything from the HA facility with notification level of notice (or lower) to all logging destinations before the third entry. The **show logging** command displays the newly inserted entry.

```
[SN5428-2A]# logging #?

[SN5428-2A]# logging #?
Index Level      Priority Facility      Route
1      critical    2          all          console vty logfile
2      debug      7          SNMP          rslog
3      warning     4          CDP           rslog

[SN5428-2A]# logging #3 level notice from HA to all

[SN5428-2A]# show logging
Logging is enabled

Index Level      Priority Facility      Route
1      critical    2          all          console vty logfile
2      debug      7          SNMP          rslog
3      notice     5          HA           all
4      warning     4          CDP          rslog

Syslog host is enabled, ip-address is 10.1.1.144
```


Related Commands	Command	Description
	clear logging table	Clear the SN 5428-2 Storage Router logging table of all entries, or to reset the table to factory defaults.
	delete logging	Delete a rule from the logging table.
	logging level	Add rule entries to route storage router event, debug and trace messages to various destinations based on facility and notification level.
	logging on	Enable or temporarily disable logging of storage router event message.
	logging syslog	Identify a remote syslog host to be used to log messages.
	save all	Save all configuration information, including the log route entries list.
	save system	Save selected system configuration information, including log route entries list.
	show logging	Display the routing rules in the logging table and the contents of the storage router log file.
	show system	Display selected system information.

logging level

To add a routing rule to the logging table, use the **logging level** command.

logging level *notification-level* **from** *facility-name* **to** *destination1* [*destination2...*]

Syntax Description	<i>notification-level</i>	Limit logging to messages of a specified level or lower levels. See Table 12-13 in the Usage Guidelines section for a list of valid names that can be used for the <i>notification-level</i> argument.
	from <i>facility-name</i>	The name of the facility. A facility is the feature area from which the message is received. See Table 12-14 in the Usage Guidelines section for a list of valid facility names. Each facility can have eight notification levels. Each notification level can have up to seven destination.
	to <i>destination1</i> [<i>destination2...</i>]	At least one of the destinations described in Table 12-15 .

Defaults

The factory default logging rules are as follows:

- All messages from all facilities at notice level or lower levels are logged to all destinations.
- All messages from all facilities at info level or lower levels are logged to the storage router log file.
- All messages from all facilities at debug level are not logged.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced

Usage Guidelines

Event, trace and debug messages can be routed to various destinations, based on the notification level of the message and the application area (facility) that generated the message. When a log message is received by the storage router, the logging table rules are searched by facility name and by notification level until a match is found. The log message is sent to all the destinations specified by the matching rule. When a new routing rule is added, it is appended to the existing list of entries.

Messages are sent in the following format:

```
<timestamp>: %<facility>-<level_number>-<mnemonic>: <message text>
```

The following is an example log message, for the SNMP facility:

```
Mar 18 11:48:05: %SNMP-5-SASAS: SnmpApp starting...
```

Each facility can have up to eight notification levels. The notification level limits logging to messages of the specified level or lower levels, based on level number. [Table 12-13](#) describes the available logging levels.

Each facility and notification level pair can have up to seven destinations. [Table 12-14](#) describes the available facility names.

Table 12-13 Logging Level Notification Levels and Corresponding Numbers

Notification Level	Level Number	Description
emergency	0	System unusable
alert	1	Immediate action needed
critical	2	Critical conditions
error	3	Error conditions
warning	4	Non-fatal warning conditions
notice	5	Normal but significant conditions
info	6	Informational messages only
debug	7	Information for troubleshooting purposes

**Note**

The debug notification level should be used for specific troubleshooting purposes only. System performance and HA behavior may be adversely affected by logging at the debug notification level.

Table 12-14 Logging Level Facilities

Facility Name	Description
all	All facilities.
AUTH	AAA authentication.
CDP	Cisco Discovery Protocol.
CONF	Configuration functions.
FC	Fibre Channel interfaces.
FCIP	FCIP functions.
GE	Gigabit Ethernet interfaces.
HA	High availability cluster functions.
IF	Interface manager.
INVALID	Generic functions.
IP	IP functions.
ISCSI	iSCSI functions.
MON	Hardware monitor.
SLP	Service Location Protocol service functions.
SNMP	Simple Network Management Protocol.
SYSLOG	Syslog functions.
UI	User interface functions.
VTP	VTP and VLAN functions.

Table 12-15 describes the available logging destinations.

Table 12-15 Logging Level Destinations

Destination	Description
all	Logs to all destinations.
none	No logging occurs.
console	Logs to console CLI sessions.
logfile	Logs messages to the storage router log file.
rslog	Logs messages to a remote syslog server. Use the logging syslog command to specify the IP address of the remote syslog server.
vty	Logs to all Telnet, SSH, or other virtual terminal CLI sessions.

Use the **save system bootconfig** or **save all bootconfig** commands to save the logging table

To delete a routing rule from the logging table, use the **delete logging** command.



Note

Any message that does not have a matching rule in the logging table is discarded.

Examples

The following example logs anything from the HA facility with notification level of notice (or lower) to all logging destinations.

```
[SN5428-2A] # logging level notice from HA to all
```

The following example logs messages from all facilities with a notification level of warning or lower to all destinations. (If this is the only rule in the logging table, any message with a notification level of debug, info or notice is discarded and not logged.) The log route entries are saved to the bootable configuration of the storage router.

```
[SN5428-2A] # logging level warning from all to all
[SN5428-2A] # save system bootconfig
```


Related Commands	Command	Description
	clear logging table	Clear the SN 5428-2 Storage Router logging table of all entries, or to reset the table to factory defaults.
	delete logging	Delete a rule from the logging table.
	logging #?	Insert a routing rule entry into the storage router logging table.
	logging on	Enable or temporarily disable logging of storage router event message.
	logging syslog	Identify a remote syslog host to be used to log messages.
	save all	Save all configuration information, including the log route entries list.
	save system	Save selected system configuration information, including log route entries list.
	show logging	Display the routing rules in the logging table and the contents of the storage router log file.
	show system	Display selected system information.

logging on

To enable logging of SN 5428-2 Storage Router event messages based on the rules in the logging table, use the **logging on** command. To temporarily disable logging of all event messages, use the **no** form of this command.

logging on

no logging on

Syntax Description

This command has no arguments or keywords.

Defaults

Logging is enabled by default. The factory default logging rules are as follows:

- All messages from all facilities at notice level or lower levels are logged to all destinations.
- All messages from all facilities at info level or lower levels are logged to the storage router log file.
- All messages from all facilities at debug level are not logged.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use the **no** form of this command to quickly disable logging of all messages. For example, if there is an error condition that is overwhelming the console with messages, enter **no logging on** to temporarily disable logging without changing the logging table. Use the **logging on** command to re-enable logging when the problem is resolved.

Examples

The following example temporarily disables logging of all event messages:

```
[SN5428-2A] # no logging on
```


Related Commands	Command	Description
	clear logging table	Clear the SN 5428-2 Storage Router logging table of all entries, or to reset the table to factory defaults.
	delete logging	Delete a rule from the logging table.
	logging #?	Insert a routing rule entry into the storage router logging table.
	logging level	Add rule entries to route storage router event, debug and trace messages to various destinations based on facility and notification level.
	logging syslog	Identify a remote syslog host to be used to log messages.
	save all	Save all configuration information, including the log route entries list.
	save system	Save selected system configuration information, including log route entries list.
	show logging	Display the routing rules in the logging table and the contents of the storage router log file.
	show system	Display selected system information.

logging syslog

To identify a remote syslog host to be used to log SN 5428-2 Storage Router event messages, use the **logging syslog** command. Use the **no** form of this command to disable remote logging.

logging syslog *A.B.C.D*

no logging syslog

Syntax Description	<i>A.B.C.D</i>	The IP address of the syslog host to be used for remote logging.
---------------------------	----------------	--

Defaults	Remote logging is disabled by default.
-----------------	--

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	This command identifies a remote syslog host to receive storage router event messages.
	<ul style="list-style-type: none">• Use the logging level command with the destination keyword rslog to configure the messages to be logged to the remote host.• Use the no logging syslog command to disable remote logging.• Use the delete logging command to remove specific logging table entries.• Use the show logging command to display the status of remote logging and the IP address of the remote syslog server.

Examples	The following example identifies the IP address of the remote syslog host as <i>10.1.1.144</i> and adds a entry to the logging table to route all emergency level messages to that remote host.
-----------------	---

```
[SN5428-2A] # logging syslog 10.1.1.144
[SN5428-2A] # logging level emergency from all to rslog
```


Related Commands	Command	Description
	clear logging table	Clear the SN 5428-2 Storage Router logging table of all entries, or to reset the table to factory defaults.
	delete logging	Delete a rule from the logging table.
	logging #?	Insert a routing rule entry into the storage router logging table.
	logging level	Add rule entries to route storage router event, debug and trace messages to various destinations based on facility and notification level.
	logging on	Enable or temporarily disable logging of storage router event message.
	save all	Save all configuration information, including the remote logging configuration.
	save system	Save selected system configuration information, including remote logging information.
	show logging	Display the routing rules in the logging table and the contents of the storage router log file.
	show system	Display selected system information.

logout

To terminate the current CLI management session, use the **logout** command.

logout

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator or Monitor.
----------------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	
	• If you are connected to the storage router in Administrator mode or Monitor mode via a Telnet or SSH session, the logout command terminates the CLI management session. No CLI commands can be issued until you log in again.
	• If you are connected to the storage router in Administrator mode via the console interface, the logout command returns the session to Monitor mode (like the exit command).
	• If you are connected to the storage router in Monitor mode via the console interface, the logout command has no effect. If console passwords are enabled, you are immediately prompted for the Monitor mode password.

Related Commands	Command	Description
	enable	Enter Administrator mode.
	exit	Leave Administrator mode and enter Monitor mode.

monitor password

To set the password used for view-only access to the SN 5428-2 Storage Router management interface, use the **monitor password** command. Access may be via Telnet or SSH (for CLI) or web-based GUI.

monitor password *string*

Syntax Description	<i>string</i>	A case-sensitive password associated with view-only access to the storage router management interface. The default password is <i>cisco</i> .
--------------------	---------------	---

Defaults	The default password is <i>cisco</i> .
----------	--

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	<p>The management interface is password protected. You must enter passwords when accessing the storage router via the CLI or web-based GUI. (Passwords can also be applied to the console interface. See the restrict console command for additional information.) The Monitor mode password provides view-only access to the management interface, while the Administrator mode password allows you to create entities and make changes to the configuration of the storage router system.</p> <p>To clear the Monitor mode password, set the password string to "", effectively setting it to nothing.</p>
------------------	---



Note

If Login authentication is enabled for the storage router, users are prompted for both a user name and a password when accessing the storage router via a console, Telnet or SSH management session.

In a cluster environment, the Administrator mode and Monitor mode passwords are cluster-wide configuration elements and apply to all storage routers in a cluster. The password management functions are handled by a single storage router. To determine which storage router is performing password management functions, issue the **show cluster** command. If you issue the **monitor password** command from a storage router that is not performing password management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Examples	<p>The following example sets the Monitor mode password to <i>M17g23</i>. All passwords are case sensitive.</p> <pre>[SN5428-2A]# monitor password M17g23</pre>
----------	--



Note

The password is displayed in clear text as the command is entered, but it is changed to a series of number signs (#####) when the change is acknowledged.

Related Commands	Command	Description
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
	aaa generate password	Generate a long random password.
	admin password	Set the login password for administrative access to the management interface.
	enable	Enter Administrator mode.
	exit	Leave Administration mode and enter Monitor mode.
	save all	Save all configuration information, including the Monitor mode password.
	save system	Save selected system information, including the Monitor mode password.
	setup access	Run the wizard to configure Monitor mode and Administrator mode passwords.

ntp peer

To specify the name or IP address of a Network Time Protocol (NTP) server with which the SN 5428-2 Storage Router will synchronize date and time, use the **ntp peer** command. To clear the current NTP server setting, use the **no** form of this command.

ntp peer{*A.B.C.D* | *server-name*}

no ntp peer

Syntax Description	<i>A.B.C.D</i>	The IP address of the NTP server with which the storage router synchronizes date and time. <i>A.B.C.D</i> is the dotted quad notation of the IP address.
	<i>server-name</i>	The name of the NTP server with which the storage router synchronizes date and time. In order to specify a server name, the storage router must be configured to use a DNS server using the ip name-server command.

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	The storage router must provide accurate date and time information for log files and user interfaces. It will use the services of the NTP server to keep the date and time synchronized with the rest of the network.
	If the NTP server is outside the storage router management subnet, use the ip route command to add an appropriate gateway IP address to the routing table.

Examples	The following example sets the IP address of the NTP server for the storage router to <i>10.1.60.86</i> .
	[SN5428-2A] # ntp peer 10.1.60.86

Related Commands	Command	Description
	clock set	Set the storage router system clock.
	clock timezone	Specify the time zone associated with the storage router.
	ip route	Add a static route to the SN 5428-2 Storage Router routing table.
	save all	Save all configuration information.
	save system	Save selected system information, including NTP server name.
	setup time	Run the wizard to configure the system date and time.
	show clock	Display the current system date and time, including the system time zone.
	show system	Display selected system information, including NTP server address.

ping

To verify communication with another SN 5428-2 Storage Router or system in the network, use the **ping** command.

ping {*ip-address* | *servername*} [**numpkts** *nn*] [**size** *sn*]

Syntax Description

<i>ip-address</i>	The IP address of another system or SN 5428-2 Storage Router.
<i>servername</i>	The name of another server. The storage router must be configured to use the services of a Domain Name Server (DNS).
numpkts <i>nn</i>	(Optional) The maximum number of pings that may be sent. The default value is five.
size <i>sn</i>	(Optional) The size of each ping packet, in bytes. The minimum size is 64 bytes; the maximum size is 4096 bytes. The default is 64 bytes.

Defaults

The default setting is to attempt five 64-byte pings.

Command Modes

Administrator or Monitor. The optional **numpkts** and **size** keywords are not available in Monitor mode.

Command History

Release	Modification
3.2.1	This command was introduced.
3.3.1	The optional numpkts and size keywords are restricted to Administrator mode only.

Usage Guidelines

Use this command to verify that there is a TCP/IP communication path to another SN 5428-2 Storage Router or system in the network.

Examples

The following example attempts to verify the communication path to the IP address 10.1.30.17, using the default size and maximum number of packets:

```
[SN5428-2A] # ping 10.1.30.17
```

The following example attempts to reach the IP address 10.1.30.17 by sending up to three pings, each consisting of a 120-byte packet. You must be logged on in Administrator mode to execute this command.

```
[SN5428-2A] # ping 10.1.30.17 numpkts 3 size 120
```

Related Commands

Command	Description
show ip	Display entries from the SN 5428-2 Storage Router routing table and statistics about the protocols used in the storage router network.

radius-server deadtime

To improve RADIUS response time when some servers might be unavailable, use the **radius-server deadtime** command to cause the storage router to skip the unavailable servers immediately. To set the dead time to 0, effectively preventing the storage router from skipping any RADIUS server, use the **no** form of this command.

radius-server deadtime *minutes*

no radius-server deadtime

Syntax Description	<i>minutes</i>	The length of time, in minutes, for which a RADIUS server is skipped over by the storage router when requesting AAA authentication services, up to a maximum of 1440 minutes (24 hours).
---------------------------	----------------	--

Defaults	The dead time is set to zero (0) by default.
-----------------	--

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	<p>Use this command to cause the storage router to mark as “dead” any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the authentication request to time out before trying the next configured server. A RADIUS server marked as dead is skipped by additional requests for the specified number of minutes, unless all RADIUS servers are marked as dead. If all RADIUS servers are marked as dead, the deadtime setting is ignored.</p> <p>This is a global command that applies to all configured RADIUS servers. To override the global dead time setting for a specific group of RADIUS server, use the aaa group server radius deadtime command.</p>
-------------------------	--

Examples	The following example specifies a dead time of five minutes for all RADIUS servers that fail to respond to AAA authentication requests:
-----------------	---

```
[SN5428-2A] # radius-server deadtime 5
```

The following example effectively sets a dead time of zero minutes for all RADIUS servers. The storage router will wait for any AAA authentication request to a RADIUS server to time out before retransmitting or retrying the next configured server.

```
[SN5428-2A] # no radius-server deadtime
```


Related Commands	Command	Description
	aaa group server radius deadtime	Specify the length of time the storage router can skip a RADIUS server in the named group that is marked as unavailable.
	show aaa	Display AAA configuration information.

radius-server host

To specify a RADIUS server to be used for AAA authentication services, use the **radius-server host** command. To delete the specified RADIUS server, use the **no** form of this command.

radius-server host *ip-address* [**auth-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*]
[**key** *key-string*]

no radius-server host *ip-address* [**auth-port** *port-number*]

Syntax Description	
<i>ip-address</i>	The IP address of the RADIUS server.
auth-port <i>port-number</i>	(Optional) The UDP destination port for authentication requests. If unspecified, the port number defaults to 1645.
timeout <i>seconds</i>	(Optional) The host-specific time interval that the storage router waits for the RADIUS server to reply before retransmitting. Enter a value in the range of 1 to 1000. This setting overrides the global value of the radius-server timeout command. If no timeout value is specified, the global value is used.
retransmit <i>retries</i>	(Optional) The number of times a RADIUS request is resent to the RADIUS server, if the server is not responding or responding slowly. Enter a value in the range of 0 to 100. A value of 0 disables RADIUS request retransmission. This setting overrides the global setting of the radius-server retransmit command. If no retransmit value is specified, the global value is used.
key <i>key-string</i>	(Optional) The authentication and encryption key for all RADIUS communications between the storage router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. If spaces are used in the key, enclose the key in quotation marks. This key overrides the global setting of the radius-server key command. If no key string is specified, the global value is used.

Defaults	No RADIUS server is specified.
-----------------	--------------------------------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

AAA authentication services are used to provide the following authentication types:

- iSCSI authentication—provides authentication of IP hosts requiring access to storage via SCSI routing instances
- Login authentication—provides authentication of users requiring Monitor mode access to the storage router via the CLI
- Enable authentication—provides authentication of users requiring Administrator mode access to the storage router via the CLI **enable** command

You can use multiple **radius-server host** commands to specify multiple RADIUS servers. AAA authentication searches for servers in the order in which you specify them.

Use the **aaa group server radius server** command to add a RADIUS server to a server group. If you delete a RADIUS server, delete the server from the RADIUS server using the **no aaa group server radius server** command.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each RADIUS server.

A retransmit value of zero (0) disables RADIUS request retransmission.

If you use spaces in the key, enclose the key in quotation marks.

**Note**

Verification of IP addresses in a server group occurs only at runtime. If a RADIUS server group contains an IP address that is not defined as a RADIUS server, the authentication process generates error messages and the IP address is skipped. This could cause unexpected authentication failures.

Examples

The following example identifies the server with IP address *10.5.0.53* as the RADIUS server and uses the default port for authentication:

```
[SN5428-2A]# radius-server host 10.5.0.53
```

The following example identifies port 1612 as the destination port for authentication requests on the RADIUS server *10.6.0.61*:

```
[SN5428-2A]# radius-server host 10.6.0.61 auth-port 1612
```

The following example identifies the server with IP address *10.5.0.53* as the RADIUS server, uses ports 1612 as the authorization port, sets the timeout value to 6, sets the retransmit value to 5, and sets “rad123” as the encryption key, matching the key on the RADIUS server:

```
[SN5428-2A]# radius-server host 10.5.0.53 auth-port 1612 timeout 6 retransmit 5 key rad123
```


Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
	aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
	aaa group server radius deadtime	Specify the length of time the storage router can skip a RADIUS server in the named group that is marked as unavailable.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	radius-server deadtime	Specify the length of time the storage router can skip a RADIUS server that is marked as unavailable.
	radius-server key	Sets the global authentication and encryption key for all RADIUS communications between the storage router and the RADIUS daemon.
	radius-server retransmit	Specifies how many times the storage router resends the RADIUS request to a server before giving up.
	radius-server timeout	Sets the interval the storage router waits for a RADIUS server to reply before retransmitting.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

radius-server key

To set the authentication and encryption key to be used for all RADIUS communications between the SN 5428-2 Storage Router and the RADIUS daemon, use the **radius-server key** command. To disable the key, use the **no** form of this command.

radius-server key *key-string*

no radius-server key

Syntax Description	<i>key-string</i>	The authentication and encryption key string to be used for all RADIUS communications, in clear text. If spaces are used in the key, enclose the key in quotation marks.
--------------------	-------------------	--

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>3.2.1</td><td>This command was introduced.</td></tr></table>	Release	Modification	3.2.1	This command was introduced.
Release	Modification				
3.2.1	This command was introduced.				

Usage Guidelines	<p>Use the radius-server key command to set the global authentication and encryption key to be used by the storage router for communications with RADIUS servers. The key entered as part of the command must match the key used on the RADIUS daemon. If the key includes spaces, enclose the key in quotation marks.</p> <p>To override the global key for a specific RADIUS server, use the radius-server host command with the key keyword.</p>
------------------	--

Examples	<p>The following example sets the global authentication and encryption key to <i>my key string</i>:</p> <pre>[SN5428-2A] # radius-server key "my key string"</pre>
----------	--

Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
	aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
	aaa group server radius deadline	Specify the length of time the storage router can skip a RADIUS server in the named group that is marked as unavailable.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	debug aaa	Enable debugging for the AAA authentication services.
	radius-server deadline	Specify the length of time the storage router can skip a RADIUS server that is marked as unavailable.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	radius-server retransmit	Specifies how many times the storage router resends the RADIUS request to a server before giving up.
	radius-server timeout	Sets the interval the storage router waits for a RADIUS server to reply before retransmitting.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

radius-server retransmit

To specify the number of times the SN 5428-2 Storage Router resends the RADIUS request to each server in the list of configured RADIUS servers after a timeout occurs, use the **radius-server retransmit** command. To disable retransmission, use the **no** form of this command.

radius-server retransmit *retries*

no radius-server retransmit

Syntax Description	<i>retries</i>	The number of times the request can be resent to each server in the list. Enter a value in the range of 0 to 100. A value of zero (0) disables RADIUS request retransmission. The default is 3.
--------------------	----------------	---

Defaults	The number of possible resends defaults to three.
----------	---

Command Modes	Administrator.
---------------	----------------

Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>3.2.1</td><td>This command was introduced.</td></tr></table>	Release	Modification	3.2.1	This command was introduced.
Release	Modification				
3.2.1	This command was introduced.				

Usage Guidelines	<p>If multiple RADIUS servers are configured for AAA authentication, the storage router attempts to reach each server in the list before incrementing the retransmit count. To disable RADIUS request retransmission, set the retransmit count to zero.</p> <p>To override the global retransmit count for a specific RADIUS server, use the radius-server host command with the retransmit keyword.</p>
------------------	--

Examples	<p>The following example sets the retransmit count to six, meaning the request can be resent up to six times for every RADIUS server:</p> <pre>[SN5428-2A] # radius-server retransmit 6</pre> <p>The following example disables RADIUS request retransmission by setting the retransmit count to zero:</p> <pre>[SN5428-2A] # radius-server retransmit 0</pre>
----------	--

Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
	aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
	aaa group server radius deadtime	Specify the length of time the storage router can skip a RADIUS server in the named group that is marked as unavailable.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	debug aaa	Enable debugging for the AAA authentication services.
	radius-server deadtime	Specify the length of time the storage router can skip a RADIUS server that is marked as unavailable.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	radius-server key	Sets the global authentication and encryption key for all RADIUS communications between the storage router and the RADIUS daemon.
	radius-server timeout	Sets the interval the storage router waits for a RADIUS server to reply before retransmitting.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

radius-server timeout

To set the global interval that the SN 5428-2 Storage Router waits for a RADIUS server to reply, use the **radius-server timeout** command. To restore the default, use the **no** form of this command.

radius-server timeout *seconds*

no radius-server timeout

Syntax Description	<i>seconds</i>	The global timeout value in seconds. Enter a value in the range of 1 to 1000. The default is 5.
--------------------	----------------	---

Defaults	The timeout value defaults to five seconds.
----------	---

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to set the number of seconds the storage router waits for a RADIUS server to reply before timing out. To override the global timeout value for a specific RADIUS server, use the radius-server host command with the timeout keyword.
------------------	---

Examples	The following example sets the global timeout value to 10. You may want to increase the timeout value if you have network problems or if the RADIUS servers are slow to response, which causes consistent timeouts when a lower timeout value is used. [SN5428-2A] # radius-server timeout 10
----------	---

Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
	aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
	aaa group server radius deadtime	Specify the length of time the storage router can skip a RADIUS server in the named group that is marked as unavailable.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	debug aaa	Enable debugging for the AAA authentication services.
	radius-server deadtime	Specify the length of time the storage router can skip a RADIUS server that is marked as unavailable.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	radius-server key	Sets the global authentication and encryption key for all RADIUS communications between the storage router and the RADIUS daemon.
	radius-server retransmit	Specifies how many times the storage router resends the RADIUS request to a server before giving up.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

read script

To read and execute the CLI commands in a command file, use the **read script** command.

```
read script command-file [force [parameters]]
```

Syntax Description	<i>command-file</i>	The name of the command file. The command file must exist in the <i>script</i> directory.
	force	(Optional) Suppress warning prompts and messages and execute the script immediately.
	<i>parameters</i>	(Optional) Pass one or more parameters to the specified script. If the parameter includes spaces, enclose it in quotation marks.

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Use the **show bootconfig** and **show runningconfig** commands with the **to** keyword to create basic files containing many of the CLI commands that were issued to create the SN 5428-2 Storage Router bootable or currently running configuration. These files can be modified and used as command files to automate common tasks.

You can also manually create a command file. If you have a set of CLI commands that you run periodically, you can place them in a command file, copy that file to the storage router *script* directory and use the **read script** command to execute them when needed.

Each command should be on a separate line or contain a backslash (\) as the line continuation character at the end of the line. At the end of a continuation sequence, add a blank line as a separator between the sequence and any following command. Any line beginning with an exclamation mark (!) or a number sign (#) is considered to be a comment and will not be executed.

When the command is issued without the **force** keyword, you are reminded that the action may change the configuration of the storage router and are then prompted to confirm your actions. When the command is issued with the force keyword, all warning prompts and messages are suppressed and the script is executed immediately.

You can also pass optional parameters to the script to control processing. Any parameter that includes spaces must be enclosed in quotation marks. Within the script, use the key character “@” to instruct the script execution function to substitute the value of the specified parameter. Whenever the execution function encounters @1, it substitutes the value of the first passed parameter. The value of the second parameter is substituted for @2, and so forth.

See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for additional information about using scripts to automate tasks.

Examples

The following example reads and executes the CLI commands in the command file named *myCommands*.

```
[SN5428-2A]# read script myCommands
*** Warning: this script may change your configuration.
Do you want to continue? [yes/no (yes)] yes
```

Related Commands

Command	Description
show bootconfig	Display the bootable configuration, or create a command file based on the bootable configuration.
show cli	Display the syntax of CLI commands.
show runningconfig	Display the running configuration, or create a command file based on the running configuration.
show script	Display the contents of the <i>script</i> directory or the contents of the named command file.

reboot

To cause the SN 5428-2 Storage Router to shut down and then restart, issue the **reboot** command.



Note

Rebooting may cause the storage router to run a different version of software. See the **software version** command for details.

reboot [force] [fast]

Syntax Description

fast	(Optional) Force a soft reboot of the storage router, bypassing hardware diagnostics.
force	(Optional) Force an immediate reboot of the storage router.

Defaults

If there are unsaved configuration changes when the command is issued, the default is to save all changes before rebooting. If the command is issued with the optional **force** keyword, any unsaved configuration changes are discarded.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

If the storage router is participating in a cluster, the **reboot** command will cause any SCSI routing instances running on this storage router to failover to another node in the cluster. At restart, the cluster determines any SCSI routing instances that should start on the storage router. If the SN 5428-2 is identified as the preferred storage router for any SCSI routing instance (via the **scsirouter primary** command), that instance will start running on the SN 5428-2 (assuming targets and critical resources are available).

If the **reboot** command is issued with no keywords and there are unsaved changes to the current configuration, you can choose to either save all changes or reboot without saving any changes.

Use the **force** keyword to cause an immediate reboot of the storage router, discarding any unsaved configuration changes. Append the optional **fast** keyword to bypass diagnostics during the reboot sequence.

Examples

The following prompt is received if you issue a **reboot** command (without the **force** keyword) when the storage router has unsaved configuration changes.

```
[SN5428-2A]# reboot
*** Warning: This will reboot the system.
Do you want to continue? [yes/no (no)] yes

Changes have been made to the current configuration of the system which
have not been saved.
yes    - all of the configuration data will be saved,
no     - modifications to the configuration data will not be saved.

Save ALL configuration data? [yes/no (yes)] yes
Halting system.....
```

The following example reboots the storage router (after prompting you to save any unsaved configuration changes) but bypasses diagnostics during the reboot process:

```
[SN5428-2A]# reboot fast
```

Related Commands

Command	Description
halt	Prepare the SN 5428-2 Storage Router to be powered down.
software version	Specify the version of software to run when the storage router is restarted.

restore aaa

To cause the AAA authentication configuration to be copied from the specified configuration file into persistent memory, use the **restore aaa** command. The configuration file must exist in the *savedconfig* directory. To display the contents of the *savedconfig* directory, issue the **show savedconfig** command.


Note

If the storage router belongs to a cluster, the restored AAA configuration information will automatically be propagated to other members of that cluster.

restore aaa from *filename*

Syntax Description

from <i>filename</i>	The name of the configuration file containing the information to be restored. This file must exist in the <i>savedconfig</i> directory.
-----------------------------	---

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The **restore** command overwrites all existing AAA configuration information, including any user name and passwords in the local username database, RADIUS and TACACS+ configuration information, and the AAA authentication lists used for iSCSI, Enable, and Login authentication.


Note

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue a **restore aaa** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions. See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about operating the storage router in a cluster.

Examples

The following example restores the AAA authentication configuration from the saved configuration file named *aaa_backup*:

[SN5428-2A]# **restore aaa from aaa_backup**

Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
	aaa generate password	Generate a long random password.
	aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
	aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	debug aaa	Enable debugging for the AAA authentication services.
	delete savedconfig	Remove a saved configuration file from the storage router.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.
	show savedconfig	List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

restore accesslist

To cause the named access list or all access lists to be copied from the specified configuration file into persistent memory, use the **restore accesslist** command. The configuration file must exist in the *savedconfig* directory. To display the contents of the *savedconfig* directory, issue the **show savedconfig** command.



Note

If the storage router belongs to a cluster, the restored access list information will automatically be propagated to other members of that cluster.

restore accesslist {*name* | **all**} **from** *filename*

Syntax Description

<i>name</i>	The name of the access list to be restored.
all	Keyword to restore all access lists.
from <i>filename</i>	The name of the configuration file containing the information to be restored. This file must exist in the <i>savedconfig</i> directory.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

If the access list currently exists in some form, the **restore** command does not delete existing information. The **restore** command adds missing entries, or overwrites existing entries of the same name, but never purges or deletes existing access list entries. If necessary, you can delete an access list and all its entries and then restore it from a saved configuration file.

There is a maximum of 100 access lists per storage router or per storage router cluster. There is a maximum of 200 access list identification entries across all access lists in the storage router or storage router cluster.



Note

In a cluster environment, access list management functions are handled by a single storage router. To determine which storage router is performing access list management functions, issue the **show cluster** command. If you issue a **restore accesslist** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the node that is currently handling those functions. See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about operating the storage router in a cluster.

Examples

The following example restores the access list named *fooList* from the saved configuration file named *accessList_backup*:

```
[SN5428-2A] # restore accesslist fooList from accessList_backup
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
restore all	Restore all the contents of the named configuration file into memory.
restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
save accesslist	Save configuration data for the named access list or for all access lists.
save scsirouter	Save configuration information for the named SCSI routing instance.
save system	Save selected system configuration information.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
show accesslist	Display the contents of the named access list or all access lists.
show savedconfig	List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file.

restore all

To cause all the previously saved configuration information to be copied from the specified configuration file into persistent memory, use the **restore all** command. The configuration file must exist in the *savedconfig* directory. Use the **show savedconfig** command to display the contents of the *savedconfig* directory.



Note

This command may change the running configuration of the storage router.

restore all from *filename*

Syntax Description

from <i>filename</i>	The name of the configuration file containing the information to be restored. This file must exist in the <i>savedconfig</i> directory.
-----------------------------	---

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The **restore all** command restores all information from the named configuration file. Depending on the information that is restored, the running configuration of the storage router may be changed.

A **restore** command may overwrite or delete existing items. However, the **restore** command will not purge or delete existing items from access lists, but will add missing items or overwrite existing items of the same name. If necessary, you may delete access lists, or any other item to be restored, before restoring from a saved configuration file.

The **restore all** command will not restore the route table and RIP settings, the Fibre Channel (FC) zoning database, or the logging table. Use the **restore system ip-route** command to restore a saved route table and RIP settings, and the **restore fcswitch zones** command to restore the FC zoning database. Use the **restore system logging** command to restore the logging table.

SCSI routing instances and FCIP instances must be stopped before they can be restored. Use the **no scsirouter enable** command to stop active SCSI routing instances. Use the **no fcip enable** command to stop an active FCIP instance. After the restore is complete, use the **scsirouter enable** command to start the restored SCSI routing instances. Restored FCIP instances are automatically restarted.

**Note**

In a cluster environment, all AAA, access list, password, and VLAN management functions are handled by a single storage router. To determine which storage router is performing these management functions, issue the **show cluster** command. If you issue the **restore all** command from a storage router that is not performing these management functions, the CLI displays an informational message with the name of the node that is currently handling those functions. See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about operating the storage router in a cluster.

Examples

The following example restores all configuration data contained in the configuration file named *foo_backup* into persistent memory:

```
[SN5428-2A]# restore all from foo_backup
```

Related Commands

Command	Description
failover scsirouter	Cause the named SCSI routing instance to cease running on the storage router.
restore aaa	Restore AAA authentication services from the named configuration file.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
restore fcswitch	Restore Fibre Channel configuration information from the named configuration file.
restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
restore system	Restore selected system information from the named configuration file.
restore vlan	Restore VLAN configuration information from the named configuration file.
save aaa	Save the current AAA configuration information.
save accesslist	Save configuration data for the named access list or all access lists.
save all	Save all configuration information.
save scsirouter	Save configuration information for the named SCSI routing instance.
save system	Save selected system configuration information.
save vlan	Save configuration information for the named VLAN or all VLANs.
scsirouter enable	Stop or start the named SCSI routing instance.
show savedconfig	List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file.

restore fcip

To cause the previously saved configuration information related to the named FCIP instance to be copied from the specified configuration file into the bootable configuration, use the **restore fcip** command. The configuration file must exist in the *savedconfig* directory. Use the **show savedconfig** command to display the contents of the *savedconfig* directory.



Note

This does not change the running configuration of the storage router.

restore fcip {*name* | **all**} **from** *filename*

Syntax Description

<i>name</i>	The name of the FCIP instance to be restored. Valid names are <i>fcip1</i> and <i>fcip2</i> .
all	Keyword to restore all FCIP instances.
from <i>filename</i>	The name of the configuration file containing the information to be restored. This file must exist in the <i>savedconfig</i> directory.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced.

Usage Guidelines

The FCIP instance should be inactive before it is restored. Use the **no fcip enable** command to stop an active FCIP instance so it can be restored. After the specified FCIP instance is restored, it is automatically enabled and the running configuration of the storage router is updated.

A **restore** command never deletes existing FCIP instances. The **restore** command will add missing instances and will overwrite configuration information for existing instances of the same name. If necessary, you can delete the FCIP instance and then restore it from a saved configuration file.

Examples

The following example restores the FCIP instance *fcip1* from the configuration file named *fcip_backup001*:

```
[SN5428-2A]# restore fcip fcip1 from fcip_backup001
```


Related Commands	Command	Description
	fcip	Create an FCIP instance.
	fcip enable	Stop or start the named FCIP instance.
	save fcip	Save configuration information for the named FCIP instance.
	show fcip	Display configuration and operational information for the named FCIP instance.

restore fcswitch

To cause the previously saved configuration information associated with the SN 5428-2 Storage Router Fibre Channel (FC) interfaces to be copied from the specified configuration file into the bootable configuration, use the **restore fcswitch** command. The configuration file must exist in the *savedconfig* directory. Use the **show savedconfig** command to display the contents of the *savedconfig* directory.

restore fcswitch {all | config | interface | zones} from *filename*

Syntax Description		
all	Keyword used to restore all global and interface-specific FC configuration information from the specified configuration file.	Note Zoning information is not restored.
config	Keyword used to restore global FC configuration information, including time out values and domain ID.	
interface	Keyword used to restore configuration information for the FC interfaces, including link speed and port type settings.	
zones	Keyword used to restore all alias, zone and zone set configuration information. If the storage router is connected to the FC switched fabric, the restored zoning database is propagated to the FC switched fabric	
from filename	The name of the configuration file containing the information to be restored. This file must exist in the <i>savedconfig</i> directory.	

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines The **restore fcswitch** command overwrites the specified FC configuration information.

Use the **config** keyword to restore global FC configuration information, including:

- The domain ID and domain ID lock setting
- Resource allocation timeout value
- Distributed services timeout value
- Fabric stability timeout value
- Error detect timeout value
- Buffer-to-buffer credit value for all FC ports
- Zoning management operational settings, including merge mode and level of communication between the storage router and devices in the fabric when there is no active zone set

Use the **interface** keyword to restore configuration information for each FC port, including:

- State of the interface (enabled or disabled)
- Fairness algorithm
- FAN
- MFS bundling and associated timeout value
- Transfer rate (linkspeed)
- Port type

Use the **zones** keyword to restore the internal zoning database, including:

- Aliases and alias members
- Zones and zone members
- Zone sets and zone set members
- Active zone set information

**Caution**

If the SN 5428-2 Storage Router is connected to the FC switched fabric, the restored zoning database information is propagated throughout the fabric.

Examples

The following example restores the configuration information for all FC interface from the configuration file named *fc_config_08152002*:

```
[SN5428-2A] # restore fcswitch interface from fc_config_08152002
```

The following example restore all global and interface-specific FC configuration information from the configuration file named *SN5428-2A_L2*:

```
[SN5428-2A] # restore fcswitch all from SN5428-2A_L2
```


Related Commands	Command	Description
	delete fcalias	Delete the named alias or the specified alias member.
	delete zone	Delete the specified Fibre Channel zone or the specified member of the zone from the zoning database.
	delete zoneset	Delete the specified zone from the zone set or to delete the entire named zone set from the zoning database.
	fcalias	Create an alias entity for use in Fibre Channel zoning.
	fcswitch domainid	Set the domain ID for the storage router, to be used for FC switched fabric zoning.
	fcswitch dstov	Specify the amount of time the storage router is to wait for Fibre Channel Distributed Services.
	fcswitch edtov	Specify an error detect timeout value for all Fibre Channel interfaces.
	fcswitch fstov	Specify the fabric stability timeout value.
	fcswitch interop-credit	Set the data buffer credit capacity for all FC ports.
	fcswitch ratov	Specify a Fibre Channel resource allocation timeout value for the storage router.
	fcswitch zoning autosave	Enable the SN 5428-2 Storage Router to save zoning changes received from switches in the fabric.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	fcswitch zoning merge	Set zoning merge compliance.
	interface fc? al-fairness	Enable the fairness algorithm on the named FC interface.
	interface fc? fan-enable	Enable Fabric Address Notification (FAN) on the named FC interface.
	interface fc? linkspeed	Set the transfer rate for the named FC interface.
	interface fc? mfs-bundle	Enable Multi-Frame Sequence bundling for the named FC interface.
	interface fc? type	Set the port type for the named FC interface.
	restore all	Restore all the contents of the named configuration file into memory.
	save fcswitch	Save all Fibre Channel configuration, including global configuration settings and zoning information.
	show fcalias	Display information about aliases and their members.
	show fcswitch	Display global configuration information for storage router FC interfaces.
	show fcswitch eport	Display FSPF protocol information.
	show interface	Display operational and configuration information for the specified interface or all interfaces.
	show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
	show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
	zone	Create a Fibre Channel fabric zone.
	zoneset	Create a Fibre Channel fabric zone set.

restore scsirouter

To cause the previously saved configuration information related to the named SCSI routing instance to be copied from the specified configuration file into the bootable configuration, use the **restore scsirouter** command. The configuration file must exist in the *savedconfig* directory. Use the **show savedconfig** command to display the contents of the *savedconfig* directory.

**Note**

This does not change the running configuration of the storage router.

restore scsirouter {*name* | **all**} **from** *filename*

Syntax Description

<i>name</i>	The name of the SCSI routing instance to be restored.
all	Keyword to restore all SCSI routing instances.
from <i>filename</i>	The name of the configuration file containing the information to be restored. This file must exist in the <i>savedconfig</i> directory.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

A SCSI routing instance must be inactive before it can be restored. Use the **no scsirouter enable** command to stop an active SCSI routing instance so it can be restored. After the specified SCSI routing instance is restored, issue the **scsirouter enable** command to start the instance and update the running configuration of the storage router.

A **restore** command never deletes existing SCSI routing instances. The **restore** command will add missing instances and will overwrite configuration information for existing instances of the same name. If necessary, you can delete a SCSI routing instance and then restore it from a saved configuration file.

Examples

The following example restores the SCSI routing instance *foo* from the configuration file named *scsi_backup001*:

```
[SN5428-2A]# restore scsirouter foo from scsi_backup001
```


Related Commands	Command	Description
	failover scsirouter	Cause the named SCSI routing instance to cease running on the storage router.
	restore accesslist	Restore the named access list or all access lists from the named configuration file.
	restore all	Restore the contents of the named configuration file into memory.
	save accesslist	Save configuration data for the named access list or all access lists.
	save all	Save all configuration information.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	scsirouter enable	Stop or start the named SCSI routing instance.
	scsirouter primary	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
	scsirouter target maxcmdqueuedepth	Specify the maximum number of commands allowed at any given time from each iSCSI session to the specified target.
	show savedconfig	List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file.

restore system

To cause previously saved system configuration information to be copied from the specified configuration file into persistent memory, use the **restore system** command. The configuration file must exist in the *savedconfig* directory. Use the **show savedconfig** command to display the contents of the *savedconfig* directory.

restore system {*name* | **all**} **from** *filename*

Syntax Description	<i>name</i>	The named system information to be restored. See Table 12-16 in the Usage Guidelines section for a list of valid names that can be used for the <i>name</i> argument.
	all	Restore all restorable system information (except the route table and RIP settings, and the logging table) from the saved configuration file. Restorable system information includes CDP configuration, administrator contact data, DNS and NTP information, restrict configuration, remote logging data, SNMP configuration, Telnet and Secure Shell (SSH) settings, and the default download location for updated storage router software.
		Note The route table, RIP settings, and the logging table, are not restored.
	from <i>filename</i>	The name of the configuration file containing the information to be restored. This file must exist in the <i>savedconfig</i> directory.

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Table 12-16 describes the named system information that can be restored.

Table 12-16 Restore System Named System Information

Named System Configuration	Description
cdp	Restore CDP configuration.
contactinfo	Restore administrator contact information.
ip-route	Restore the route table and RIP settings.
logging	Restore the routing rules in the storage router event message logging table. Restored rules are appended to the end of the table.
name-server	Restore DNS configuration.
ntp	Restore NTP server configuration.
remotelog	Restore IP address of host used for remote logging.
restrict	Restore the storage router restrict configuration.
snmp	Restore SNMP configuration.
software	Restore the default software download location and user name and password information for HTTP, proxy, and TFTP.
ssh	Restore the Secure Shell (SSH) configuration information.
telnet	Restores the session timeout value for Telnet and SSH management sessions.

Some system information that is saved when the **save system** command is issued is not available for restoration from a saved configuration file. Use the **show savedconfig** command to display the contents of the specified configuration file. The following configuration information is available for display but cannot be restored:

- Management and HA interface IP addresses
- Gigabit Ethernet interface configuration information
- Administrator mode and Monitor mode passwords
- HA configuration mode

Examples

The following example restores all restorable system configuration information (except the route table and the logging table) from the saved configuration file *system_backup*:

```
[SN5428-2A]# restore system all from system_backup
```

The following example restores the route table and RIP settings from the saved configuration file *system_backup*:

```
[SN5428-2A]# restore system ip-route from system_backup
[SN5428-2A]# restore system rip from system_backup
```


The following example restores the logging table from the saved configuration file *system_backup*:

```
[SN5428-2A] # restore system logging from system_backup
```

The following example restores the SNMP configuration information from the saved configuration file *sys_SN5428-2A*:

```
[SN5428-2A] # restore system snmp from sys_SN5428-2A
```

Related Commands

Commands	Description
delete savedconfig	Remove a saved configuration file from the storage router.
restore all	Restore the contents of the named configuration file into memory.
save all	Save all configuration information.
save system	Save selected system configuration information.
show savedconfig	List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file.

restore vlan

To cause the specified VLAN to be copied from the named configuration file into persistent memory, use the **restore vlan** command. The configuration file must exist in the *savedconfig* directory. To display the contents of the *savedconfig* directory, issue the **show savedconfig** command.



Note

If the SN 5428-2 Storage Router belongs to a cluster, the restored VLAN configuration information will automatically be propagated to other members of that cluster.

restore vlan {*vid* | **all**} **from** *filename*

Syntax Description

<i>vid</i>	The VLAN identification number.
all	Restore all VLAN definitions.
from <i>filename</i>	The name of the configuration file containing the information to be restored. This file must exist in the <i>savedconfig</i> directory.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

If the VLAN currently exists, the **restore vlan** command overwrites existing configuration information with the information from the named configuration file. The **restore vlan** command also restores the VTP configuration information.



Note

In a cluster environment, VLAN management functions are handled by a single storage router. To determine which storage router is performing VLAN management functions, issue the **show cluster** command. If you issue a **restore vlan** command from a storage router that is not performing VLAN management functions, the CLI displays an informational message with the name of the node that is currently handling those functions. See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about operating the storage router in a cluster.

Examples

The following example restores VLAN *100* from the *vlanBackup* file:

```
[SN5428-2A] # restore vlan 100 from vlanBackup
```


Related Commands	Command	Description
	save vlan	Save configuration information for the named VLAN or all VLANs
	scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
	show savedconfig	List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file.
	show vlan	Display configuration and operational information for the specified VLAN or all VLANs.
	show vtp	Display configuration and operational information for VTP.
	vlan	Configure a non-VTP VLAN on the storage router.
	vtp domain	Assign a VTP domain name to the storage router.
	vtp mode	Configure the storage router to operate in client or transparent VTP mode.

restrict

To close access to the specified interface via the named service, use the **restrict** command. To allow access via the named service, use the **no** form of this command.

restrict all [*service*]

restrict interface {*service* | **all**}

no restrict all [*service*]

no restrict interface {*service* | **all**}

Syntax Description

<i>interface</i>	Restrict access to the specified interface. See Table 12-17 in the Usage Guidelines section for a list of interface names.
<i>service</i>	Restrict access via the specified service or protocol. See Table 12-18 in the Usage Guidelines section for a list of service names.
all	Restrict all interfaces or all services.

Defaults

The following are factory default settings:

- FTP using port 21 is restricted on all interfaces.
- HTTP using port 80 is allowed on the management and HA interfaces. It is restricted on the Gigabit Ethernet interfaces.
- Remote login (rlogin) using port 513 is restricted on all interfaces.
- SNMP using port 161 is allowed on the management interface only. It is restricted on the HA and Gigabit Ethernet interfaces.
- SSH using port 22 is allowed on the management interface only. It is restricted on the HA and Gigabit Ethernet interfaces.
- SSL using port 443 is restricted on all interfaces.
- Telnet using port 23 is allowed on the management interface only. It is restricted on the HA and Gigabit Ethernet interfaces.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use the **restrict** command to restrict unauthorized access to storage router interfaces. Use the **show restrict** command to display the current interface and service restrictions.

You can restrict access on the interfaces listed in [Table 12-17](#).

Table 12-17 restrict interface

Interface Keyword	Description
ge?	The Gigabit Ethernet interfaces (including all logical interfaces created by associating a VLAN with a Gigabit Ethernet IP address for a SCSI routing instance). All services are restricted on the Gigabit Ethernet interfaces by default.
ha	The HA interface. This interface is open to HTTP by default.
mgmt	The management interface. This interface is open to Telnet, HTTP, SNMP and SSH by default.

You can restrict access to the storage router interfaces by the services or protocols, shown in [Table 12-18](#).

Table 12-18 restrict interface service

Service Keyword	Description
ftp	File Transfer Protocol. FTP access is restricted on all interfaces, by default.
http	Hypertext Transfer Protocol. HTTP access is available on the management and HA interfaces, by default.
rlogin	Remote login on port 513. If rlogin is enabled for an interface, the setting is only valid until the storage router is restarted. The rlogin setting is not retained across a storage router restart; rlogin returns to a restricted state for all interfaces. Note Rlogin is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.
ssh	Secure Shell. SSH can be used as a replacement for Telnet and remote login. SSH is enabled on the management interface by default; it is restricted on all other interfaces. Note The SSH service is started, by default. Use the no ssh enable command to stop the SSH service (disabling access via SSH) without changing the restrict settings.
snmp	Simple Network Management Protocol. SNMP is enabled on the management interface by default.

Table 12-18 restrict interface service (continued)

Service Keyword	Description
ssl	Secure Socket Layer. SSL is restricted on all interfaces by default.
telnet	<p>Telnet. Telnet access is enabled on the management interface by default; it is restricted on all other interfaces.</p> <p>Note The Telnet server is started by default. Use the no telnet enable command to stop the Telnet server (disabling access via Telnet) without changing the restrict settings.</p>

To access the GUI using an SSL connection, enable SSL on the appropriate interface and change the URL to use “https” instead of “http.”

To completely disable the SN 5428-2 GUI, restrict HTTP access to all interfaces.

Examples

The following example restricts HTTP access to the management interface, preventing access to the web-based GUI from this interface:

```
[SN5428-2A] # restrict mgmt http
```

The following example restricts Telnet access to the HA interface:

```
[SN5428-2A] # restrict ha telnet
```

The following example restricts access to all interfaces via FTP.

```
[SN5428-2A] # restrict all ftp
```

The following example enables SSL on the management interface.

```
[SN5428-2A] # no restrict mgmt ssl
```

The following example enables SSH on the Gigabit Ethernet interface, *ge1*:

```
[SN5428-2A] # no restrict ge1 ssh
```

Related Commands

Command	Description
restrict console	Enable or disable password checking on the console interface.
show restrict	Display configurable security settings for the storage router interfaces.
ssh enable	Enable SSH and start the SSH service.
ssh keygen	Generate a Secure Shell (SSH) public and private key pair for the storage router.
telnet enable	Enable Telnet and start the Telnet server.

restrict console

To enable password checking on the SN 5428-2 Storage Router console interface, use the **restrict console** command. The Administrator mode and Monitor mode passwords will be required when accessing the storage router via a console connected to the EIA/TIA-232 port. To disable password checking on the console interface, use the **no** form of this command.

restrict console

no restrict console

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	Passwords are disabled on the console interface.
-----------------	--

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command if you need to restrict access to the console interface.
-------------------------	---

Examples	The following example enables password checking on the console interface: [SN5428-2A] # restrict console
-----------------	--

Related Commands	Command	Description
	restrict	Secure access to storage router interfaces by communications protocols and services.
	show restrict	Display configurable security settings for the storage router interfaces.

save aaa

To save the current AAA settings to nonvolatile memory, use the **save aaa** command.

```
save aaa {filename | bootconfig}
```

Syntax Description	<i>filename</i>	The name of the file where the AAA configuration information will be written. This file is stored in the <i>savedconfig</i> directory.
	bootconfig	Save the AAA settings to the bootable configuration, which is used when the SN 5428-2 Storage Router is restarted. If the storage router belongs to a cluster, the saved AAA settings will automatically be propagated to other members of that cluster.

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

You must save configuration data from the running configuration to the bootable configuration for it to be retained in the storage router when it is restarted. Use the *filename* parameter to save the AAA configuration to a file. Configurations saved to a file can be moved between storage routers and can be restored at a later time.

The following information is saved:

- The AAA authentication lists
- The username database
- All RADIUS server configuration information (including server groups)
- All TACACS+ server configuration information (including server groups)



Note

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **save aaa** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions. See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about operating the storage router in a cluster.

Examples

The following example saves the running AAA settings to the bootable configuration, used when the storage router is restarted:

```
[SN5428-2A] # save aaa bootconfig
```

The following example saves the running AAA settings to a file named *aaa_SN5428-2A*:

```
[SN5428-2A] # save aaa aaa_SN5428-2A
```

Related Commands

Command	Description
aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
aaa test authentication	Enable testing of the specified AAA authentication list.
debug aaa	Enable debugging for the AAA authentication services.
delete savedconfig	Remove a saved configuration file from the storage router.
radius-server host	Configure remote RADIUS servers for AAA authentication services.
restore aaa	Restore AAA authentication services from the named configuration file.
save accesslist	Save configuration data for the named access list or for all access lists.
save all	Save all configuration information.
save scsirouter	Save configuration information for the named SCSI routing instance.
save system	Save selected system configuration information.
save vlan	Save configuration information for the named VLAN or all VLANs.
scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
show aaa	Display AAA configuration information.
show savedconfig	List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file.
tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.
username password	Add a user name and optional password to the local username database.

save accesslist

To save configuration data to nonvolatile memory for the named accesslist or for all access lists, use the **save accesslist** command.

save accesslist {*name* | **all**} {*filename* | **bootconfig**}

Syntax Description

<i>name</i>	The name of the access list to be saved.
all	Save all access lists.
<i>filename</i>	The name of the file where the running access list configuration data will be written. This file is stored in the <i>savedconfig</i> directory.
bootconfig	Save the access list from the running configuration to the bootable configuration, used when the SN 5428-2 Storage Router is restarted. If the storage router belongs to a cluster, the saved access list information will automatically be propagated to other members of that cluster.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

You must save configuration data from the running configuration to the bootable configuration for it to be retained in the storage router when it is restarted. Configurations saved to a file can be moved between storage routers, and can be restored at a later time.

There is a maximum of 100 access lists per storage router or per storage router cluster. There is a maximum of 200 access list identification entries across all access lists in the storage router or storage router cluster.



Note

In a cluster environment, access list management functions are handled by a single storage router. To determine which storage router is performing access list management functions, issue the **show cluster** command. If you issue the **save accesslist** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the node that is currently handling those functions. See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about operating the storage router in a cluster.

Examples

The following example saves the current configuration for all access lists to the bootable configuration, used when the storage router is restarted:

```
[SN5428-2A] # save accesslist all bootconfig
```

The following example saves the access list *fooList* to a configuration file named *fooList_SN5428-2A*:

```
[SN5428-2A] # save accesslist fooList fooList_SN5428-2A
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
delete savedconfig	Remove a saved configuration file from the storage router.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
save aaa	Save the current AAA configuration information.
save all	Save all configuration information.
save scsirouter	Save configuration information for the named SCSI routing instance.
save system	Save selected system configuration information.
save vlan	Save configuration information for the named VLAN or all VLANs.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
show accesslist	Display the contents of the named access list or all access lists.
show savedconfig	List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file.

save all

To save all configuration data for the SN 5428-2 Storage Router to nonvolatile memory, use the **save all** command.

```
save all {filename | bootconfig}
```


Syntax Description	<i>filename</i>	The name of the file where the configuration data will be written. This file is stored in the <i>savedconfig</i> directory.
	bootconfig	Save the current running configuration information to the bootable configuration, used when the SN 5428-2 Storage Router is restarted. If the storage router belongs to a cluster, any saved cluster elements will automatically be propagated to other members of that cluster.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines You must save configuration data from the running configuration to the bootable configuration for it to be retained in the storage router when it is restarted. Depending on the deployment, the **save all** command saves AAA configuration, SCSI routing instances, FCIP instances, access lists, VLANs, global Fibre Channel (FC) settings and FC interface configurations, and selected system configuration information. Configurations saved to a file can be moved between storage routers and can be restored at a later time.


Note

In a cluster environment, all AAA, access list, password, and VLAN management functions are handled by a single storage router. To determine which storage router is performing these management functions, issue the **show cluster** command. If you issue the **save all** command from a storage router that is not performing these management functions, the CLI displays an informational message with the name of the node that is currently handling the functions. See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about operating the storage router in a cluster.

Examples The following example saves the current running configuration to the bootable configuration:

```
[SN5428-2A]# save all bootconfig
```


The following example saves the current running configuration to the file named *SN5428-2A_03Nov2001*. You may want to do this as a means of archiving the current running configuration of the storage router on a regular basis.

```
[SN5428-2A] # save all SN5428-2A_03Nov2001
```

Related Commands	Command	Description
	delete savedconfig	Remove a saved configuration file from the storage router.
	restore all	Restore the contents of the named configuration file into memory.
	save aaa	Save current AAA configuration information.
	save accesslist	Save configuration data for the named access list or for all access lists.
	save fcip	Save configuration information for the named FCIP instance.
	save fcswitch	Save all Fibre Channel configuration, including global configuration settings and zoning information.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	save system	Save selected system configuration information.
	save vlan	Save configuration information for the named VLAN or all VLANs.
	show savedconfig	List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file.

save fcip

To save all configuration data associated with the named FCIP instance to nonvolatile memory, use the **save fcip** command.

save fcip {*name* | **all**} {*filename* | **bootconfig**}

Syntax Description

<i>name</i>	The name of the FCIP instance. Valid names are <i>fcip1</i> and <i>fcip2</i> .
all	Save configuration data for all FCIP instances.
<i>filename</i>	The name of the file where the configuration data will be written. This file is stored in the <i>savedconfig</i> directory.
bootconfig	Save the FCIP instance from the running configuration to the bootable configuration, used when the SN 5428-2 Storage Router is restarted.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Maintenance
3.3.1	This command was introduced.

Usage Guidelines

You must save configuration data from the running configuration to the bootable configuration for it to be retained in the storage router when it is restarted. Configurations saved to a file can be moved between storage routers and can be restored at a later time.

Examples

The following example saves all FCIP instances currently running on this SN 5428-2 to the bootable configuration, used when the storage router is restarted:

```
[SN5428-2A] # save fcip all bootconfig
```

The following example saves the FCIP instance named *fcip1* to the file named *fcip_SN5428-2A*:

```
[SN5428-2A] # save fcip fcip1 fcip_SN5428-2A
```

Related Commands

Command	Description
fcip	Create an FCIP instance.
fcip enable	Stop or start the named FCIP instance.
restore fcip	Restore the named SCSI routing instance from the named configuration file.
show fcip	Display configuration and operational information for the named FCIP instance.

save fcswitch

To save all configuration data for the SN 5428-2 Storage Router Fibre Channel (FC) interfaces to nonvolatile memory, use the **save fcswitch** command.

save fcswitch {*filename* | **bootconfig**}

Syntax Description	<i>filename</i>	The name of the file where the configuration data will be written. This file is stored in the <i>savedconfig</i> directory.
	bootconfig	Save the FC configuration from the running configuration to the bootable configuration, used when the SN 5428-2 Storage Router is restarted.

Defaults	None.
-----------------	-------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	You must save configuration data from the running configuration to the bootable configuration for it to be retained in the storage router when it is restarted. Configurations saved to a file can be moved between storage routers and can be restored at a later time.
-------------------------	--

Examples	The following example saves all the FC configuration information to the bootable configuration, used when the storage router is restarted:
-----------------	--

```
[SN5428-2A] # save fcswitch bootconfig
```

The following example saves all the FC configuration information to the file named *fc_SN5428-2A*:

```
[SN5428-2A] # save fcswitch fc_SN5428-2A
```


Related Commands	Command	Description
	delete fcalias	Delete the named alias or the specified alias member.
	delete zone	Delete the specified Fibre Channel zone or the specified member of the zone from the zoning database.
	delete zoneset	Delete the specified zone from the zone set or to delete the entire named zone set from the zoning database.
	fcalias	Create an alias entity for use in Fibre Channel zoning.
	fcswitch domainid	Set the domain ID for the storage router, to be used for FC switched fabric zoning.
	fcswitch dstov	Specify the amount of time the storage router is to wait for Fibre Channel Distributed Services.
	fcswitch edtov	Specify an error detect timeout value for all Fibre Channel interfaces.
	fcswitch fstov	Specify the fabric stability timeout value.
	fcswitch interop-credit	Set the data buffer credit capacity for all FC ports.
	fcswitch ratov	Specify a Fibre Channel resource allocation timeout value for the storage router.
	fcswitch zoning autosave	Enable the SN 5428-2 Storage Router to save zoning changes received from switches in the fabric.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	fcswitch zoning merge	Set zoning merge compliance.
	interface fc? al-fairness	Enable the fairness algorithm on the named FC interface.
	interface fc? fan-enable	Enable Fabric Address Notification (FAN) on the named FC interface.
	interface fc? linkspeed	Set the transfer rate for the named FC interface.
	interface fc? mfs-bundle	Enable Multi-Frame Sequence bundling for the named FC interface.
	interface fc? type	Set the port type for the named FC interface.
	restore fcswitch	Restore Fibre Channel configuration information from the named configuration file.
	show fcalias	Display information about aliases and their members.
	show fcswitch	Display global configuration information for storage router FC interfaces.
	show fcswitch eport	Display FSPF protocol information.
	show interface	Display operational and configuration information for the specified interface or all interfaces.
	show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
	show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
	zone	Create a Fibre Channel fabric zone.
	zoneset	Create a Fibre Channel fabric zone set.

save scsirouter

To save all configuration data associated with the named SCSI routing instance to nonvolatile memory, use the **save scsirouter** command.

save scsirouter {*name* | **all**} [*filename* | **bootconfig**]

Syntax Description	<i>name</i>	The name of the SCSI routing instance.
	all	Save configuration data for all SCSI routing instances.
	<i>filename</i>	The name of the file where the configuration data will be written. This file is stored in the <i>savedconfig</i> directory.
	bootconfig	Save the SCSI routing instance from the running configuration to the bootable configuration, used when the SN 5428-2 Storage Router is restarted.

Defaults	None.
-----------------	-------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Maintenance
	3.2.1	This command was introduced.

Usage Guidelines

You must save configuration data from the running configuration to the bootable configuration for it to be retained in the storage router when it is restarted. Configurations saved to a file can be moved between storage routers and can be restored at a later time.

In a cluster environment, the SCSI routing instance can only be saved on the node that is currently running that instance.

Examples

The following example saves all SCSI routing instances currently running on this SN 5428-2 to the bootable configuration, used when the storage router is restarted:

```
[SN5428-2A]# save scsirouter all bootconfig
```

The following example saves the SCSI routing instance named *foo* to the file named *foo_SN5428-2A*:

```
[SN5428-2A]# save scsirouter foo foo_SN5428-2A
```


Related Commands	Commands	Description
	delete savedconfig	Remove a saved configuration file from the storage router.
	delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
	restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
	save aaa	Save the current AAA configuration information.
	save accesslist	Save configuration data for the named access list or all access lists.
	save all	Save all configuration information.
	save system	Save selected system configuration information.
	save vlan	Save configuration information for the named VLAN or all VLANs.
	scsirouter	Create a SCSI routing instance.
	scsirouter enable	Stop or start the named SCSI routing instance.
	scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
	scsirouter target maxcmdqueuedepth	Specify the maximum number of commands allowed at any given time from each iSCSI session to the specified target.
	setup scsi	Run the wizard to configure a SCSI routing instance.
	show savedconfig	List the contents of the savedconfig directory or the contents of the named configuration file.
	show scsirouter	Display configuration and operational information for the named SCSI routing instance.

save system

To save selected system configuration information to nonvolatile memory, use the **save system** command.

save system {*filename* | **bootconfig**}

Syntax Description	<i>filename</i>	The name of the file where the system configuration data will be written. This file is stored in the <i>savedconfig</i> directory.
	bootconfig	Save the current running system configuration to the bootable configuration, used when the SN 5428-2 Storage Router is restarted.

Defaults	None.
-----------------	-------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

You must save configuration data from the running configuration to the bootable configuration for it to be retained in the storage router when it is restarted. Configurations saved to a file can be moved between storage routers and can be restored at a later time.

The following system configuration data is saved:

- Monitor and Administrator passwords
- Administrative contact information
- Network Time Protocol (NTP) server name
- Primary and optional secondary Domain Name Server (DNS)
- Default location for downloading storage router software
- System and cluster name
- Management and high availability (HA) interface addresses
- Static routes
- RIP settings
- SNMP settings
- CDP settings
- Restrict settings
- IP address of remote syslog host for logging
- Logging table

- Configuration information for the Gigabit Ethernet interfaces
- Management session timeout value
- Secure Shell (SSH) settings

Examples

The following example saves the current system configuration to the bootable configuration, used when the storage router is restarted:

```
[SN5428-2A] # save system bootconfig
```

The following example copies the current system configuration to the file named `sys_SN5428-2A`:

```
[SN5428-2A] # save system sys_SN5428-2A
```

Related Commands

Commands	Description
delete savedconfig	Remove a saved configuration file from the storage router.
hostname	Specify the storage router system name.
restore system	Restore selected system information from the named configuration file.
save aaa	Save the current AAA configuration information.
save accesslist	Save configuration data for the named access list or all access lists.
save all	Save all configuration information.
save scsirouter	Save configuration information for the named SCSI routing instance.
save vlan	Save configuration information for the named VLAN or all VLANs.
show savedconfig	List the contents of the savedconfig directory or the contents of the named configuration file.
show system	Display selected system information, including system name.

save vlan

To save VLAN and VTP configuration information for the specified VLAN or for all VLANs to nonvolatile memory, use the **save vlan** command.

save vlan {*vid* | **all**} [*filename* | **bootconfig**]

Syntax Description

<i>vid</i>	The VLAN identification number of the VLAN configuration to be saved.
all	Save all VLANs associated with this storage router.
<i>filename</i>	The name of the file where the current VLAN configuration data will be written. This file is stored in the <i>savedconfig</i> directory.
bootconfig	Save the current VLAN configuration to the system's bootable configuration, to be used when the storage router is restarted. If the storage router belongs to a cluster, the saved VLAN information will automatically be propagated to other members of that cluster.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

You must save configuration data from the running configuration to the bootable configuration for it to be retained in the storage router when it is restarted. Configurations saved to a file can be moved between storage routers and can be restored at a later time.

VTP mode and domain information is saved, along with the specified VLAN configuration information.



Note

In a cluster environment, VLAN management functions are handled by a single storage router. To determine which storage router is performing VLAN management functions, issue the **show cluster** command. If you issue the **save vlan** command from a storage router that is not performing VLAN management functions, the CLI displays an informational message with the name of the node that is currently handling those functions. See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about operating the storage router in a cluster.

The following example saves the current configuration for all VLANs to the system's bootable configuration, to be used when the storage router is restarted:

```
[SN5428-2A] # save vlan all bootconfig
```

The following example saves VLAN 12 to the file named *vlanbackup*:

```
[SN5428-2A] # save vlan 12 vlanbackup
```


Related Commands	Command	Description
	restore vlan	Restore VLAN configuration information from the named configuration file.
	save aaa	Save current AAA configuration information.
	save accesslist	Save configuration data for the named access list or all access lists.
	save all	Save all configuration information.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	save system	Save selected system configuration information.
	show savedconfig	List the contents of the <i>savedconfig</i> directory or the contents of the named configuration file.
	show vlan	Display configuration and operational information for the specified VLAN or all VLANs.
	show vtp	Display configuration and operational information for VTP.
	vlan	Configure a non-VTP VLAN on the storage router.
	vtp domain	Assign a VTP domain name to the storage router.
	vtp mode	Configure the storage router to operate in client or transparent VTP mode.

scsirouter

To create a SCSI routing instance, use the **scsirouter** command.

scsirouter *name*

Syntax Description	<i>name</i>	The name of the SCSI routing instance created by this command. Enter a maximum of 31 characters.
--------------------	-------------	--

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines SCSI routing is the routing of SCSI requests and responses between IP hosts in an IP network and storage devices in a Fibre Channel storage network. The SCSI routing instance becomes a binding point for the association of other configuration parameters. A SCSI routing instance provides IP hosts access to Fibre Channel storage.

There can be a maximum of 12 SCSI routing instances defined per storage router; if the storage router is a member of a cluster, no more than 12 instances can be defined across the cluster.

**Note**

If the storage router is deployed for transparent SCSI routing, there can be only one SCSI routing instance. The SCSI routing instance is named *transparent* and is automatically created during initial system configuration.

Examples The following command creates a SCSI routing entity named *myCompanyWebserver2*.

```
[SN5428-2A] # scsirouter myCompanyWebserver2
```


Related Commands	Command	Description
	accesslist	Create an access list entity.
	delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
	failover scsirouter	Cause the named SCSI routing instance to cease running on the storage router.
	restore accesslist	Restore the named access list or all access lists from the named configuration file.
	restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
	save accesslist	Save configuration data for the named access list or all access lists.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	scsirouter enable	Stop or start the named SCSI routing instance.
	scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
	setup scsi	Run the wizard to configure a SCSI routing instance.
	show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter authentication

To enable iSCSI authentication using the specified AAA authentication services for the named SCSI routing instance, use the **scsirouter authentication** command.

scsirouter *name* **authentication** {*listname* | **default** | **none**}

Syntax Description

<i>name</i>	The name of this SCSI routing instance.
<i>listname</i>	Enable AAA authentication using the specified iSCSI authentication list.
default	Enable AAA authentication using the default iSCSI authentication list.
none	Disable AAA authentication for this SCSI routing instance.

Defaults

AAA authentication is disabled.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use the **scsirouter authentication** command to enable iSCSI authentication for IP hosts requesting access to storage using the named SCSI routing instance. AAA performs authentication using the services configured on the specified iSCSI authentication list. Use the **aaa authentication iscsi** command to configure the iSCSI authentication list.



Note

If authentication is enabled for a SCSI routing instance using the *default* iSCSI authentication list, but no AAA authentication list is available, AAA attempts to use the “local” authentication method. If a list other than default is specified and not available, AAA authentication will fail for the SCSI routing instance.

Examples

The following example enables iSCSI authentication for the SCSI routing instance named *foo*, using the default iSCSI authentication list:

```
[SN5428-2A] # scsirouter foo authentication default
```

The following example enables iSCSI authentication of the SCSI routing instance named *foo2*, using the iSCSI authentication list named *testlab*:

```
[SN5428-2A] # scsirouter foo2 authentication testlab
```


Related Commands	Command	Description
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	debug aaa	Enable debugging for the AAA authentication services.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.
	username password	Add a user name and optional password to the local username database.

scsirouter cdbretrycount

To specify the number of times a failed command should be retried before returning an error on the CDB, use the **scsirouter cdbretrycount** command.

scsirouter *name* **cdbretrycount** *nn*

Syntax Description

<i>name</i>	The name of this SCSI routing instance.
<i>nn</i>	The number of CDB retries. <i>nn</i> is an integer from 0 to 512. The default value is 6. There is one second between retries.

Defaults

The number of CDB retries is 6, by default.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to change the number of times a failed CDB will be retried by the storage router before returning an error on the CDB. Retries occur every second. For example, with the default retry count value of 6, it would take 6 seconds before a failed command would be returned with an error.

If an intelligent storage array includes multiple paths between hosts and storage, lowering the CDB retry count value could change the triggering of failover situations.



Note

In a high availability cluster, the storage router may fail over a SCSI routing instance when some or all devices accessed through that instance cannot be reached, before the maximum number of CDB retries occurs.

Examples

The following example sets the CDB retry count value to 10:

```
[SN5428-2A] # scsirouter transparent cdbretrycount 10
```

Related Commands

Command	Description
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter description

To add user-defined identification information to the named SCSI routing instance, use the **scsirouter description** command.

scsirouter *name* **description** "*user text*"

Syntax Description

<i>name</i>	The name of this SCSI routing instance.
" <i>user text</i> "	User-defined identification information associated with this SCSI routing instance. If the string contains spaces, enclose it in quotes. Enter a maximum of 64 characters.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The **scsirouter description** command allows you to add a new description or change an existing description. Descriptions are site-specific.

Examples

The following example adds the description "Access to WebServer4 WebServer5" to the SCSI routing instance *foo1*:

```
[SN5428-2A]# scsirouter foo1 description "Access to WebServer4 WebServer5"
```

Related Commands

Command	Description
delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
save scsirouter	Save configuration information for the named SCSI routing instance.
scsirouter	Create a SCSI routing instance.
scsirouter enable	Stop or start the named SCSI routing instance.
scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
setup scsi	Run the wizard to configure a SCSI routing instance.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter enable

To start the named SCSI routing instance on this SN 5428-2 Storage Router, use the **scsirouter enable** command. To stop the named SCSI routing instance, use the **no** form of this command.

scsirouter {*name* | **all**} **enable**

no scsirouter {*name* | **all**} **enable**

Syntax Description

<i>name</i>	The name of the SCSI routing instance to be started.
all	Start all SCSI routing instances on this storage router.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

SCSI routing instances are automatically started by the storage router during the creation process, when the storage router is restarted, and when they are failed over to another storage router in a cluster. Use this command to manually control the running state of SCSI routing instances; for example, when a SCSI routing instance is restored from a saved configuration file.

SCSI routing instances that are in a stopped state are not running anywhere in the cluster. To restart a stopped SCSI routing instance, use the **scsirouter enable** command. Use the **all** keyword to start all instances on the SN 5428-2. All instances previously stopped on this storage router or available instances not running elsewhere in the cluster will start on this SN 5428-2.

The SCSI routing instance can only be started from the storage router on which it was stopped. A stopped SCSI routing instance is no longer known to any other storage router in the cluster.

Use the **scsirouter enable** command to bring a restored SCSI routing instance into the running configuration. A restored instance must be started before you can make any additional configuration changes to that instance.

Examples

The following example starts the SCSI routing instance named *foo2*. This instance must have been previously stopped.

```
[SN5428-2A] # scsirouter foo2 enable
```

The following example stops all SCSI routing instances running on the storage router:

```
[SN5428-2A] # no scsirouter all enable
```


Related Commands	Command	Description
	delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
	failover scsirouter	Cause the named SCSI routing instance to cease running on the storage router.
	restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	scsirouter	Create a SCSI routing instance.
	scsirouter primary	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
	scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
	setup scsi	Run the wizard to configure a SCSI routing instance.
	show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter failover

To build a list of storage routers to be used for failover purposes, use the **scsirouter failover** command.

scsirouter *name* **failover** {**primary** | **secondary**} *sysname*

Syntax Description

<i>name</i>	The name of the SCSI routing instance.
primary <i>sysname</i>	The name of the storage router in the cluster. In case of failure, the specified SCSI routing instance will be failed over to this storage router.
secondary <i>sysname</i>	(Optional) The name of the storage router in the cluster. If the primary storage router in the list cannot run the SCSI routing instance, it will be failed over to this storage router.
Note	Because a high availability cluster consists of two storage routers, this parameter is not used.

Defaults

None. By default, the HA failover list is not populated.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use the **scsirouter failover** command to build a list of storage routers that will be used during the failover process. If the specified SCSI routing instance fails over, the cluster attempts to start running the instance on the storage router designated as the *primary* in the HA failover list. If that storage router cannot run the SCSI routing instance, the cluster will attempt to start the instance on the storage router designated as the *secondary* in the HA failover list.

If there is no primary or secondary storage router on the HA failover list when the SCSI routing instance fails over, the cluster uses normal failover algorithms to determine where the SCSI routing instance should run.

The storage routers specified as primary and secondary should be active in the cluster when the command is issued. If the specified storage router is not currently active in the cluster, the setting will not take effect until the node is added to the cluster and the SCSI routing instance is restarted.

Use the **clear scsirouter failover** command to remove the current primary or secondary storage router from the HA failover list.



Note

This command causes the SCSI routing instance configuration information to be saved and all nodes in the cluster to be updated.

Examples

The following example builds the HA failover list for the SCSI routing instance named *foo*. The primary storage router in the HA failover list is *SN5428-2A*.

```
[SN5428-2A]# scsirouter foo failover primary SN5428-2A
```

Related Commands

Command	Description
clear scsirouter failover	Remove the designated primary or secondary storage router from the HA failover list for the specified SCSI routing instance.
delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
failover scsirouter	Cause the named SCSI routing instance to cease running on the storage router.
restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
save scsirouter	Save configuration information for the named SCSI routing instance.
scsirouter	Create a SCSI routing instance.
scsirouter enable	Stop or start the named SCSI routing instance.
scsirouter primary	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
setup scsi	Run the wizard to configure a SCSI routing instance.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter lun reset

To specify that “LUN reset” rather than “clear task” commands will be sent to the storage resources opened by the specified SCSI routing instance, use the **scsirouter lun reset** command.

scsirouter *name* **lun reset** {**yes** | **no**}

Syntax Description

<i>name</i>	The name of the SCSI routing instance. The specified SCSI routing instance must be running.
yes	Send “lun reset” to storage resources when they are opened.
no	Send “clear task” to storage resources when they are opened.

Defaults

The default is to send “clear task” commands to storage resources.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

It is preferable to send “LUN reset” commands if the device supports them. The specified SCSI routing instance must be running.

Examples

The following example enables “LUN resets” to all storage resources opened by the SCSI routing instance *foo2*:

```
[SN5428-2A] # scsirouter foo2 lun reset yes
```


Related Commands	Command	Description
	delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
	restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	scsirouter	Create a SCSI routing instance.
	scsirouter enable	Stop or start the named SCSI routing instance.
	scsirouter primary	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
	scsirouter reserveproxy	Enable the SCSI reserve/release commands for the specified SCSI routing instance and specify whether these commands are forwarded to the storage resource.
	scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
	setup scsi	Run the wizard to configure a SCSI routing instance.
	show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter password

To assign a password to a SCSI routing instance for iSCSI authentication purposes, use the **scsirouter password** command.

scsirouter *name* **password** {*password-string* | **none**}

Syntax Description		
<i>name</i>		The name of the SCSI routing instance.
<i>password-string</i>		The password associated with the named SCSI routing instance. If the password is encrypted (starts with “9”), enter a maximum of 170 characters. If the password is unencrypted (starts with “0”), enter a maximum of 66 characters. If the password is entered as an unencrypted text string, enter a maximum of 64 characters.
none		Keyword, removing any existing iSCSI password assigned to the named SCSI routing instance.

Defaults None.

Command Modes Administrator

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use this command to assign a password to the SCSI routing instance for two-way iSCSI authentication. Two-way iSCSI authentication allows authentication of the IP host and also allows the IP host, acting as an iSCSI initiator, to require authentication of the SCSI routing instance, acting as an iSCSI target. The user name and password assigned to the SCSI routing instance are used by the IP host for iSCSI authentication purposes.

iSCSI authentication must be enabled for the named SCSI routing instance. If iSCSI authentication is not enabled, the user name and password assigned to the SCSI routing instance will not be used.

The following rules apply to passwords:

- Passwords are entered in clear text. However, they are changed to “XXXXXX” in the CLI command history cache, and are stored in the local username database in an encrypted format.
- If the password contains embedded spaces, enclose it with single or double quotes.
- After initial entry, passwords display in their encrypted format. Use the **show scsirouter** command to display the SCSI routing instance authentication information. The following is an example display:

```

SCSI Router Authentication Information
Router      Authentication Username      Password
-----
zeus        web1          zeus_lab1    9 ea9bb0c57ca4806d3555f3f78a4204177a

```


The initial “9” in the example display indicates that the password is encrypted.

- You can re-enter an encrypted password using the normal **scsirouter password** command. Enter the encrypted password in single or double quotes, starting with 9 and a single space. For example, copying and pasting `password "9 ea9bb0c57ca4806d3555f3f78a4204177a"` from the example above into the **scsirouter mars password** command would assign the SCSI routing instance *mars* the same iSCSI password as the SCSI routing instance *zeus*. This functionality allows passwords to be restored from saved configuration files.
- When entering a password, a zero followed by a single space indicates that the following string is not encrypted; 9 followed by a single space indicates that the following string is encrypted. To enter a password that starts with 9 or zero, followed by one or more spaces, enter a zero and a space and then enter the password string. For example, to enter the password “0 123” for the SCSI routing instance *zeus*, enter this command:

```
scsirouter zeus password "0 0 123"
```

To enter the password “9 73Zjm 5” for SCSI routing instance *lab3*, use this command:

```
scsirouter lab3 password '0 9 73Zjm 5'
```

Examples

The following example enables iSCSI authentication, using the default authentication list, for the SCSI routing instance named *lab3* and assigns a user name of *lab3-admin* and a password of *testing* to the instance for two-way authentication:

```
[SN5428-2A]# scsirouter lab3 authentication default
* [SN5428-2A]# scsirouter lab3 username lab3-admin
* [SN5428-2A]# scsirouter lab3 password testing
```

Related Commands

Command	Description
scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
scsirouter username	Assign a user name to a SCSI routing instance for iSCSI authentication purposes.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter primary

To assign the specified system as the preferred storage router for the named SCSI routing instance, use the **scsirouter primary** command.

scsirouter *name* **primary** *sysname*

Syntax Description

<i>name</i>	The name of this SCSI routing instance.
primary <i>sysname</i>	The system name of the preferred storage router.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

At any given time, a SCSI routing instance can run on only one node in a cluster. If a SCSI routing instance has the **primary** attribute set, the specified storage router will take over running that instance upon system restart or whenever target and critical resources are available.

If the **primary** attribute is not set, the SCSI routing instance continues running on the node where it was started until it is explicitly stopped (via a **no scsirouter enable** command), it automatically fails over to another node in the cluster because targets or critical resources are unavailable, or an explicit **failover scsirouter** command is issued. This is the default behavior.

Use the **scsirouter primary** command if you always want the specified SCSI routing instance to run on a specific storage router in a cluster whenever that node is available (assuming target and critical resources are available). Use the **clear scsirouter primary** command to remove the currently configured primary value for the named SCSI routing instance.



Note

Setting the **primary** attribute saves the SCSI routing instance configuration and circulates those changes to the high availability cluster. If the specified storage router is available to the cluster and has all target and critical resources available, the SCSI routing instance will be immediately failed over. If the specified storage router is not available to the cluster, failover will occur as soon as that storage router becomes available to the cluster (assuming target and critical resources are available).

See [Chapter 10, “Configuring a High Availability Cluster,”](#) and [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about HA, cluster configuration, and managing SCSI routing instances in a cluster environment.

Examples

The following command designates the SN 5428-2 *LabRouter1* as the storage router on which the SCSI routing instance named *foo* will always, under normal conditions, run.

```
[SN5428-2A] # scsirouter foo primary LabRouter1
```

Related Commands

Command	Description
clear scsirouter primary	Remove the storage router configured as the primary for the named SCSI routing instance.
delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
save scsirouter	Save configuration information for the named SCSI routing instance.
scsirouter	Create a SCSI routing instance.
scsirouter enable	Stop or start the named SCSI routing instance.
scsirouter failover	Add the storage router to the HA failover list for the specified SCSI routing instance.
scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
setup scsi	Run the wizard to configure a SCSI routing instance.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter reserveproxy

To configure the SCSI routing instance to track SCSI reserve/release commands and to specify whether these commands are forwarded to the storage target, use the **scsirouter reserveproxy** command.

scsirouter *name* **reserveproxy** {**enable passthru** {**yes** | **no**} | **disable**}

Syntax Description

<i>name</i>	The name of the SCSI routing instance.
enable passthru yes	Configure the SCSI routing instance to track SCSI reserve and release commands and enable forwarding of these commands to storage resources.
enable passthru no	Configure the SCSI routing instance to track SCSI reserve and release commands but disable forwarding of these commands to storage resources.
disable	Disable the reserve proxy feature for the named SCSI routing instance. The storage router does not track the SCSI reserve and release commands, which are sent from the IP host. The IP host manages the SCSI reserve and release commands.

Defaults

Reserve-proxy passthru is disabled.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The SCSI reserve/release command allows an initiator to reserve the storage for its own use. Attempts to access the storage from other initiators are rejected until the first initiator releases the storage. If the reserve proxy feature is enabled using the **scsirouter reserveproxy** command, the storage router keeps track of the reserved status of target LUNs and returns the appropriate SCSI command status to other initiators that issue SCSI commands to that target LUN.

If passthru is enabled, the storage router forwards the SCSI reserve and release commands to the device. If passthru is not enabled, the SCSI reserve and release commands are not forwarded, but the storage router will respond as if the commands had been forwarded.



Note

This functionality does not apply to operating systems (such as Windows NT) which do not utilize the SCSI Reserve command.

Examples

The following example configures the SCSI routing instance *foo2* to track SCSI reserve and release commands and enables forwarding of these commands to storage resources:

```
[SN5428-2A]# scsirouter foo2 reserveproxy enable passthru yes
```


Related Commands	Command	Description
	delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
	restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	scsirouter	Create a SCSI routing instance.
	scsirouter enable	Stop or start the named SCSI routing instance.
	scsirouter failover	Add the storage router to the HA failover list for the specified SCSI routing instance.
	scsirouter lun reset	Configure the named SCSI routing instance to send a “LUN reset” command when opening all targets.
	scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
	setup scsi	Run the wizard to configure a SCSI routing instance.
	show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter serverif

To assign a Gigabit Ethernet interface and IP address to the named SCSI routing instance, use the **scsirouter serverif** command. The specified interface allows IP hosts access to Fibre Channel storage.

scsirouter name serverif ge? {*A.B.C.D/bits* | *A.B.C.D/1.2.3.4*} [**secondary ge?**]

scsirouter name serverif ge? vlan vid {*A.B.C.D/bits* | *A.B.C.D/1.2.3.4*} [**secondary ge?**]

Syntax Description	
<i>name</i>	Name of the SCSI routing instance to which you are adding the Gigabit Ethernet interface.
serverif ge?	The name of the interface. When you type the scsirouter serverif command, followed by ? , the CLI lists the interfaces available. You cannot specify a nonexistent interface.
<i>A.B.C.D/bits</i>	The IP address of the named interface. If the keyword vlan is used, the IP address is part of the specified VLAN. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style. Note The IP address must be on a unique subnet; you cannot configure an IP address that is on the same subnet as another storage router network interface.
<i>A.B.C.D/1.2.3.4</i>	The IP address of the named interface. If the keyword vlan is used, the IP address is part of the specified VLAN. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask. Note The IP address must be on a unique subnet; you cannot configure an IP address that is on the same subnet as another storage router network interface.
secondary ge?	(Optional) The name of the Gigabit Ethernet interface to be used as a secondary interface for the specified IP address. If the primary interface goes down and remains down for two seconds, the specified IP address will be moved to the secondary interface.
vlan vid	The keyword and the VLAN identifier.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

The specified interface IP address is configured on IP hosts requiring access to storage resources through the SN 5428-2 Storage Router.

Each SCSI routing instance requires two active elements:

- The *serverif* element assigns an interface and IP address for use by IP hosts requiring access to storage resources. The instance becomes active when this interface is added. A SCSI routing instance can have multiple *serverif* elements; one IP address per logical interface can be configured for a SCSI routing instance.
- The *target* element is a complex item that specifies the mapping between LUNs on the storage devices and the host systems.

The **scsirouter serverif vlan** command is used to associate a VLAN with a SCSI routing instance. All traffic using the specified Gigabit Ethernet interface will be considered as part of the VLAN; all IP hosts accessing storage through the SN 5428-2 using the specified Gigabit Ethernet interface IP address must connect as part of the specified VLAN.

When the SCSI routing instance is started, a logical interface (for example, ge2VLAN100) is created, which incorporates the physical interface and the VID. This logical interface can be displayed via the **show interface** command.

If the **secondary** keyword is used, both Gigabit Ethernet interfaces must be connected to the same network segment. If the primary interface goes down and remains down for two seconds, the IP address will be moved to the secondary interface.

**Note**

If you configure a Gigabit Ethernet IP address with a secondary interface, all Gigabit Ethernet IP addresses on the same subnet must also be configured with the same secondary interface.

Examples

The following command adds the Gigabit Ethernet interface *ge1*, with the IP address 10.1.10.128/24, to the SCSI routing instance named *foo2*.

```
[SN5428-2A] # scsirouter foo2 serverif ge1 10.1.10.128/24
```

The following command adds the Gigabit Ethernet interface *ge2* and VLAN ID 45, with IP address 10.1.30.128/24, to the SCSI routing instance *fooA*. If the primary interface is not available, the IP address will be moved to the secondary Gigabit Ethernet interface, *ge1*. The Gigabit Ethernet interfaces must be connected to the same network.

```
[SN5428-2A] # scsirouter fooA serverif ge2 vlan 45 10.1.30.128/24 secondary ge1
```

Related Commands

Command	Description
delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
save scsirouter	Save configuration information for the named SCSI routing instance.
scsirouter	Create a SCSI routing instance.
scsirouter enable	Stop or start the named SCSI routing instance.
setup scsi	Run the wizard to configure a SCSI routing instance.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter slp enable

To enable the advertisement of the targets of the named SCSI routing instance with the Service Location Protocol (SLP) service, use the **scsirouter slp enable** command. To disable target advertisement, use the **no** form of this command.

scsirouter *name* **slp enable**

no **scsirouter** *name* **slp enable**

Syntax Description

<i>name</i>	Name of the SCSI routing instance. All targets associated with this SCSI routing instance are advertised with the SLP service.
-------------	--

Defaults

Advertising with the SLP Service is enabled for all targets.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

SLP is an IP protocol designed to make it easy for network clients to discover available services on a network and to learn about the configuration of those services. By default, SLP advertisement is enabled when:

- A SCSI routing instance is started by the storage router during the creation process.
- The storage router is restarted.
- A SCSI routing instance is failed over to another storage router in a cluster.

Use this command to manually disable and re-enable the advertisement of targets with the SLP service. When target advertisement is disabled, all existing targets for the specified SCSI routing instance are de-registered, and any new targets that are added will not be advertised.

Examples

The following example disables target advertisement for the SCSI routing instance named *foo* and deregisters all of its previously registered targets from the SLP service:

```
[SN5428-2A] # no scsirouter foo slp enable
```

The following example re-enables target advertisement for the SCSI routing instance named *foo*:

```
[SN5428-2A] # scsirouter foo slp enable
```


■ scsirouter slp enable

Related Commands	Command	Description
	show slp	Display the status of the SLP service and the interface address where the SLP service is listening for incoming SLP service requests.
	slp findattrs	Discover the attributes of a specific SLP registered service.
	slp findsrvs	Locate a SLP registered service of a specific type on the local subnet.
	slp findsrvtypes	Discover all SLP registered service types on the local subnet.

scsirouter target accesslist

To associate the named access list with the specified target, use the **scsirouter target accesslist** command.

scsirouter *name* **target** {*name* | **all**} **accesslist** {*name* | **any** | **none**} [**ro** | **rw**]

Syntax Description

<i>name</i>	The name of the SCSI routing instance to which this target belongs.
target <i>name</i>	The name of the storage target to associate with this access list. The target must already exist.
target all	Associate all targets with the named access list.
accesslist <i>name</i>	The name of the access list to associate with this storage target.
accesslist any	Allow connections and logins for the specified target from any IP host. This is effectively “open access.”
accesslist none	Prevent any new connections or logins to this target from any IP hosts. This is effectively “no access.”
ro	(Optional) Allow the IP hosts identified by the specified access list read-only device access.
rw	(Optional) Allow the IP hosts identified by the specified access list read/write device access. This is the default.

Defaults

If access type (read-only or read/write) is not specified, the default is read/write.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

An access list identifies the IP hosts allowed to access the associated storage target through the SN 5428-2 Storage Router. IP hosts can be identified by IP address, CHAP user name, or iSCSI Name. Access lists are associated with specific storage targets. Each target can be associated with one access list that provides IP hosts read/write device access and one access list that provides read-only device access.

When an IP host attempts to access a storage resource, the storage router first looks for a matching entry using the access list configured to allow read/write device access. If the IP host does not have a matching entry in the read/write access list, the access list configured for read-only device access (if any) is used. If the IP host does not have a matching entry on either access list, the IP host is denied access to the storage resource.



Note

Some host operating systems impose restrictions on the use of read-only access lists. For details, see the readme files and *Release Notes for Cisco iSCSI Driver* for your IP host operating system.

- Use the **target all** form of this command to create an association between the specified access list and all targets.
- Use the reserved access list name **none** to remove any access list associations for the specified target. This effectively prevents access to this storage target from any IP host.
- Use the reserved access list name **any** to allow access to this storage target from any IP host. This is effectively “open access.”
- Existing connections and logins are not affected by an access list change. However, if there are existing connections, the storage router issues a warning message with that information in response to this command.

**Note**

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

Examples

The following example creates an association between the storage target *webserver4* (accessed via SCSI routing instance *foo*) and the access list *webserver2*. By default, the IP hosts identified by the *webserver2* access list will be allowed read/write device access to the target.

```
[SN5428-2A]# scsirouter foo target webserver4 accesslist webserver2
```

The following example provides the IP hosts identified in the access list named *media* read-only access to all targets accessed via SCSI routing instance *LabA*:

```
[SN5428-2A]# scsirouter LabA target all accesslist media ro
```

**Note**

Some host operating systems impose restrictions on the use of read-only access lists. For details, see the readme files and *Release Notes for Cisco iSCSI Driver* for your IP host operating system.

The following example provides the IP hosts identified by the access list *webcheck* read-only device access, and provides the IP hosts identified by access list *webserver2* read/write device access, to the target *webserver3*:

```
[SN5428-2A]# scsirouter foo target webserver3 accesslist webcheck ro
Setting read-only accesslist to 'webcheck' for scsirouter 'foo' target 'webserver3'
*[SN5428-2A]# scsirouter foo target webserver3 accesslist webserver2 rw
Setting read-write accesslist to 'webserver2' for scsirouter 'foo' target 'webserver3'
```


Related Commands	Command	Description
	accesslist	Create an access list entity.
	accesslist A.B.C.D/bits	Add IP addresses to an access list.
	accesslist chap-username	Add CHAP user name entries to an access list.
	accesslist iscsi-name	Add iSCSI Name entries to an access list.
	delete accesslist	Delete a specific access list entry or an entire access list.
	delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
	restore accesslist	Restore the named access list or all access lists from the named configuration file.
	restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
	save accesslist	Save configuration data for the named access list or all access lists.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	scsirouter	Create a SCSI routing instance.
	scsirouter enable	Stop or start the named SCSI routing instance.
	scsirouter primary	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
	scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
	scsirouter target crc	Control the usage of iSCSI cyclical redundancy check (CRC) on the specified target or all targets.
	setup scsi	Run the wizard to configure a SCSI routing instance.
	show accesslist	Display the contents of the named access list or all access lists.
	show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter target crc

To control the usage of iSCSI cyclical redundancy check (CRC) on the specified target or all targets, use the **scsirouter target crc** command.

scsirouter *name* **target** {*name* | **all**} **crc** {**always** | **any** | **never** | **prefer-off** | **prefer-on**}

Syntax Description

<i>name</i>	The name of the SCSI routing instance to which this target belongs.
target <i>name</i>	The name of the storage target.
target all	Apply the specified iSCSI CRC usage to all targets associated with this SCSI routing instance.
always	Always force iSCSI CRC on the target.
any	The target supports both CRC and non-CRC modes. The use of CRC is negotiated to the initiator preference.
never	The use of iSCSI CRC is disabled on this target.
prefer-off	The use of iSCSI CRC is not the preferred mode of operation for this target, but the target will negotiate the mode if CRC mode is the only mode supported by the initiator. This is the default setting.
prefer-on	The use of iSCSI CRC is the preferred mode of operation for this target, but the target will function in non-CRC mode if it is the only mode supported by the initiator.

Defaults

iSCSI CRC is not the preferred mode of operation for the target.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

CRC codes are shortened cyclic codes used for error detection. A target configured for iSCSI CRC as the preferred mode of operation (prefer-on) opts for data integrity over performance. A target configured for non-CRC mode as the preferred mode of operation (prefer-off) opts for performance over data integrity.

Depending on the initiator and target configurations, the usage of iSCSI CRC is negotiated. [Table 12-19](#) lists the CRC negotiation outcomes for each possible pair of CRC configurations.

Table 12-19 iSCSI CRC Negotiation Outcomes

Initiator CRC Mode	Target CRC Mode	CRC Negotiation Outcome
always	always	CRC is enabled.
	never	Negotiation is rejected. No session is established to the target.
	prefer-on	CRC is enabled.
	prefer-off	CRC is enabled.
	any	CRC is enabled.
never	always	Negotiation is rejected. No session is established to the target.
	never	CRC is disabled.
	prefer-on	CRC is disabled.
	prefer-off	CRC is disabled.
	any	CRC is disabled.
prefer-on	always	CRC is enabled.
	never	CRC is disabled.
	prefer-on	CRC is enabled.
	prefer-off	CRC is disabled.
	any	CRC is enabled.
prefer-off	always	CRC is enabled.
	never	CRC is disabled.
	prefer-on	CRC is enabled.
	prefer-off	CRC is disabled.
	any	CRC is disabled.

Examples

The following example configures the storage target *webserver4*, accessed through SCSI routing instanced *foo*, to always use iSCSI CRC:

```
[SN 5428-2A] # scsirouter foo target webserver4 crc always
```

The following example configures all storage targets accessed through SCSI routing instances *lab2*, to prefer the use of iSCSI CRC:

```
[SN 5428-2A] # scsirouter lab2 target all crc prefer-on
```


Related Commands	Command	Description
	delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
	restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
	scsirouter target enable	Allow or disallow connections and logins for the named target.
	show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter target description

To add a description to the named target, use the **scsirouter target description** command.

scsirouter *name* **target** *name* **description** "*user text*"

Syntax Description	<i>name</i>	The name of the SCSI routing instance to which this target belongs.
	target <i>name</i>	The name of the storage target.
	<i>"user text"</i>	User-defined identification information associated with this storage target. If the description contains spaces, enclose the string in quotes. Enter a maximum of 64 characters.

Defaults	None.
-----------------	-------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Target description information is an optional attribute of a SCSI routing instance. Use the show scsirouter command to display target description information.
-------------------------	---

Examples	The following example adds a description to the storage target <i>webserver4</i> , accessed through the SCSI routing instance <i>foo</i> :
-----------------	--

```
[SN5428-2A] # scsirouter foo target webserver4 description "Web databases"
```


Related Commands	Command	Description
	accesslist	Create an access list entity.
	accesslist A.B.C.D/bits	Add IP addresses to an access list.
	accesslist chap-username	Add CHAP user name entries to an access list.
	accesslist iscsi-name	Add iSCSI Name entries to an access list.
	delete accesslist	Delete a specific access list entry or an entire access list.
	delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
	restore accesslist	Restore the named access list or all access lists from the named configuration file.
	restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
	save accesslist	Save configuration data for the named access list or all access lists.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	scsirouter	Create a SCSI routing instance.
	scsirouter enable	Stop or start the named SCSI routing instance.
	scsirouter primary	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
	scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
	scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
	setup scsi	Run the wizard to configure a SCSI routing instance.
	show accesslist	Display the contents of the named access list or all access lists.
	show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter target enable

To allow connections and logins for the named target, use the **scsirouter target enable** command. To disallow connections and logins for the named target, use the **no** form of this command.

scsirouter *name* **target** {*name* | **all**} **enable**

no scsirouter *name* **target** {*name* | **all**} **enable**

Syntax Description	<i>name</i>	The name of the SCSI routing instance to which this target belongs.
	target <i>name</i>	The name of the storage target.
	target all	Allow connections for all targets of this SCSI routing instance to be enabled or disabled.

Defaults	None.
-----------------	-------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

When you add a target to a SCSI routing instance, it is by default enabled. However, no access list is associated with the target, thus effectively preventing any access to the storage target from any IP hosts. When you associate an access list with a target, the specified connections and logins are allowed.

Use this command to control access without changing the target access list association.

Existing connections and logins are not affected by the **no** form of this command, but future connections and logins are not allowed. If existing IP hosts are connected, the storage router issues a warning message with that information in response to this command.

Use the reserved target name **all** to enable or disable connections for all targets of this SCSI routing instance.

**Note**

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

Examples

The following example enables connections for all targets of the SCSI routing instance *foo*.

```
[SN5428-2A]# scsirouter foo target all enable
```

The following examples disables connections for the target *webservices2* of the SCSI routing instance named *lab2*:

```
[SN5428-2A]# no scsirouter lab2 target webservices2 enable
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
accesslist chap-username	Add CHAP user name entries to an access list.
accesslist iscsi-name	Add iSCSI Name entries to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
save scsirouter	Save configuration information for the named SCSI routing instance.
scsirouter	Create a SCSI routing instance.
scsirouter enable	Stop or start the named SCSI routing instance.
scsirouter primary	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
scsirouter target maxcmdqueuedepth	Specify the maximum number of commands allowed at any given time from each iSCSI session to the specified target.
setup scsi	Run the wizard to configure a SCSI routing instance.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter target {lunid | serial | wwpn} #?

To use an index method of mapping a logical target or a logical target and LUN combination to storage, use the **scsirouter target {serial | lunid | wwpn} #?** command. This command creates an indexed list of storage resources, assigning a unique index number to each LUN available. Specify the storage resources to map by using the appropriate index numbers.

scsirouter name target name wwpn #?

scsirouter name target name [lun nn] wwpn #?

scsirouter name target name lun nn {serial | lunid} #?

scsirouter name target name wwpn #nn [wwpn #nn]

scsirouter name target name lun nn wwpn #nn [wwpn #nn] [force]

scsirouter name target name lun nn {serial | lunid} #nn [force]

Syntax Description

name	Name of the SCSI routing instance to which you are adding the storage target.
target name	A user-specified name of the logical target. Enter a maximum of 31 characters or a valid iSCSI Name. There is a maximum of 100 targets per storage router or per high availability cluster.
lun nn	The LUN number associated with the logical target. The LUN number is optional if mapping to a World Wide Port Name (WWPN) address type. The LUN number is required if mapping to a serial number or LUN identifier.
#?	Request an indexed list of storage resources available on the Fibre Channel (FC) network.
serial	Use the serial number for the named storage resource. The storage resource must support unique serial numbers for each LUN.
wwpn	Use the World Wide Port Name (WWPN) address type for the named storage resource. You can specify a primary and optional secondary WWPN.
lunid	Use the unique LUN identifier, assigned when the LUN is discovered by the FC interface.
#nn	The index number from the displayed list. The storage resource listed after the number specified is the physical storage address to which the logical target or logical target and LUN combination is to be mapped.
force	(Optional) Keyword used to allow LUN-mapping of the same storage array control LUNs in multiple targets.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

This command can be used for target-only or target-and-LUN mapping.

When you map a target using WWPN and the target needs to be accessed in a high availability cluster, you must specify both the primary WWPN (the WWPN of the storage resource as known to the first storage router in the cluster) and the secondary WWPN (the WWPN of the storage resource as known to the second storage router in the cluster).

To display the indexed list of storage resources, use the number sign (#) character followed by a question mark (?). That action will cause a list of devices discovered on the FC network to display as a numbered (indexed) table. The original command is re-displayed at the prompt below the list to the point of the # keyword. Complete the command by entering the appropriate index number.

When a target is added, it is by default enabled. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts. Use the **scsirouter target accesslist** command to enable access to this storage target for selected IP hosts. See [Chapter 6, “Configuring SCSI Routing,”](#) for more information about configuring SCSI routing on the SN 5428-2 Storage Router.

**Note**

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

Use the **force** keyword to allow target-and-LUN mapping of the same storage array control LUN in multiple targets. Do not use the **force** keyword to LUN-map the same data LUN in multiple targets. LUN-mapping of the same LUN in multiple targets is advised for a control LUN on a storage controller only.

Examples

The following example displays an indexed list of storage resources available to SCSI routing instance *lab2* and maps the logical target *webserver8* to the WWPN storage address represented by index number 2.

```
[SN5428-2A]# scsirouter lab2 target webserver8 wwpn #?
```

Id	I/F	WWPN	Lun	Device		
				Type	Vendor	Product
1	fc1	2200001026448a0d	0	Disk	SEAGATE	ST217340FC
2	fc1	22000003be3203bc	0	Disk	SEAGATE	ST217341FC

```
*[SN5428-2A]# scsirouter lab2 target webserver8 wwpn #2
```


Related Commands	Command	Description
	accesslist	Create an access list entity.
	accesslist A.B.C.D/bits	Add IP addresses to an access list.
	accesslist chap-username	Add CHAP user name entries to an access list.
	accesslist iscsi-name	Add iSCSI Name entries to an access list.
	delete accesslist	Delete a specific access list entry or an entire access list.
	delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
	restore accesslist	Restore the named access list or all access lists from the named configuration file.
	restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
	save accesslist	Save configuration data for the named access list or all access lists.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	scsirouter	Create a SCSI routing instance.
	scsirouter enable	Stop or start the named SCSI routing instance.
	scsirouter primary	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
	scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
	scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
	scsirouter target enable	Allow or disallow connections and logins for the named target.
	setup scsi	Run the wizard to configure a SCSI routing instance.
	show accesslist	Display the contents of the named access list or all access lists.
	show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter target lun lunid

To map a logical target and LUN combination to a unique LUN identifier, use the **scsirouter target lun lunid** command. The **scsirouter target lun lunid** command is a target-and-LUN mapping method of mapping a logical target to storage.

```
scsirouter name target name lun nn lunid lun-identifier [force]
```

Syntax Description	name	Name of the SCSI routing instance to which you are adding the storage target.
	target name	A user-specified name of the logical target. Enter a maximum of 31 characters or a valid iSCSI Name. There is a maximum of 100 targets per storage router or per high availability cluster.
	lun nn	The LUN number associated with the logical target. LUNs are integers between 0 and 255.
	lunid lun-identifier	Use the unique LUN identifier, assigned when the LUN is discovered by the Fibre Channel interface. Enter either 16 or 32 hex digits.
	force	(Optional) Keyword used to allow LUN-mapping of the same storage array control LUNs in multiple targets.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

The **scsirouter target lun lunid** command specifies a logical target name and LUN number combination to be mapped to a physical LUN by its unique LUN identifier. The LUN identifier is represented by 16 or 32 hex digits. The digits may be separated by colons.

When a target is added, it is by default enabled. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts. Use the **scsirouter target accesslist** command to enable access to this storage target for selected IP hosts.

See [Chapter 6, “Configuring SCSI Routing,”](#) for more information about configuring SCSI routing instances on the SN 5428-2 Storage Router.



Note

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from [Cisco.com](#).

Use the **force** keyword to allow mapping of the same storage array control LUN in multiple targets. Do not use the **force** keyword to LUN-map the same data LUN in multiple targets. LUN-mapping of the same LUN in multiple targets is advised for a control LUN on a storage controller only.

Examples

The following example maps a logical target and LUN combination for SCSI router instance *foo*. The logical target and LUN combination, *webserver5* LUN 5, is mapped to the physical LUN represented by the LUN identifier *200000203719129d*.

```
[SN5428-2A] # scsirouter foo target webserver5 lun 5 lunid 220000203719129d
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
accesslist chap-username	Add CHAP user name entries to an access list.
accesslist iscsi-name	Add iSCSI Name entries to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
save scsirouter	Save configuration information for the named SCSI routing instance.
scsirouter	Create a SCSI routing instance.
scsirouter enable	Stop or start the named SCSI routing instance.
scsirouter primary	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
scsirouter target enable	Allow or disallow connections and logins for the named target.
setup scsi	Run the wizard to configure a SCSI routing instance.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter target lun serial

To map a logical target and LUN combination to the serial number of the physical LUN, use the **scsirouter target lun serial** command. The **scsirouter target lun serial** command is a target-and-LUN mapping method of mapping a logical target and LUN combination to a physical storage resource by the LUN serial number.

scsirouter *name* **target** *name* **lun** *nn* **serial** *serial_number* [**force**]

Syntax Description

<i>name</i>	Name of the SCSI routing instance to which you are adding the storage target.
target <i>name</i>	A user-specified name of the logical target. Enter a maximum of 31 characters or a valid iSCSI Name. There is a maximum of 100 targets per storage router or per high availability cluster.
lun <i>nn</i>	The LUN number associated with the target (the iSCSI LUN). iSCSI LUNs are integers between 0 and 255.
serial <i>serial_number</i>	The serial number of the physical LUN. The storage resource must support unique serial numbers for each LUN.
force	(Optional) Keyword used to allow LUN-mapping of the same storage array control LUNs in multiple targets.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The **scsirouter target lun serial** command requires both a logical target and LUN combination and the serial number of the physical LUN.

When a target is added, it is by default enabled. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts. Use the **scsirouter target accesslist** command to enable access to this storage target for selected IP hosts.

See [Chapter 6, “Configuring SCSI Routing,”](#) for more information about configuring SCSI routing instances on the SN 5428-2 Storage Router.



Note

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

Use the **force** keyword to allow mapping of the same storage array control LUN in multiple targets. Do not use the **force** keyword to LUN-map the same data LUN in multiple targets. LUN-mapping of the same LUN in multiple targets is advised for a control LUN on a storage controller only.

Examples

The following example maps the logical target and LUN combination for SCSI routing instance *lab2*. The logical target and LUN combination, *webserver9* LUN *1*, is mapped to the physical LUN with a serial number of *ST318451FC3CC05T3N00007116DLWQ*.

```
[SN5428-2A] # scsirouter lab2 target webserver9 lun 1 serial ST318451FC3CC05T3N00007116DLWQ
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
accesslist chap-username	Add CHAP user name entries to an access list.
accesslist iscsi-name	Add iSCSI Name entries to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
save scsirouter	Save configuration information for the named SCSI routing instance.
scsirouter	Create a SCSI routing instance.
scsirouter enable	Stop or start the named SCSI routing instance.
scsirouter primary	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
scsirouter target enable	Allow or disallow connections and logins for the named target.
setup scsi	Run the wizard to configure a SCSI routing instance.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter target lun wwpn lun

To map a logical target and LUN combination to a primary (and optional secondary) storage address where each storage address is specified by World Wide Port Name (WWPN) and LUN, use the **scsirouter target lun wwpn lun** command. The **scsirouter target lun wwpn lun** command is a target-and-LUN mapping method of mapping a logical target to storage.

```
scsirouter name target name lun nn wwpn xxxxxxxxxxxxxxxx lun nn
[wwpn xxxxxxxxxxxxxxxx lun nn] [force]
```

Syntax Description		
<i>name</i>		Name of the SCSI routing instance to which you are adding the storage target.
target name		A user-specified name of the logical target. Enter a maximum of 31 characters or a valid iSCSI Name. There is a maximum of 100 targets per storage router or per high-availability cluster.
lun nn		The first instance is the LUN number associated with the target (the iSCSI LUN). iSCSI LUNs are integers between 0 and 255. The second instance is the LUN number associated with the primary WWPN (physical device LUN). Physical LUNs may be any physical device number, for example 0x51d1 or 123.
wwpn xxxxxxxxxxxxxxxx		Specify a WWPN for the primary storage address. In a high availability cluster, this is the WWPN for the storage resource as known to the first storage router in the cluster.
wwpn xxxxxxxxxxxxxxxx		(Optional) Specify a WWPN for the secondary storage address, used as an alternate for mapping if the primary is not available. In a high availability cluster, this is the WWPN for the storage resource as known to the second storage router in the cluster.
lun nn		(Optional) Specify the LUN associated with the optional secondary WWPN. Physical LUNs may be any physical device number, for example 0x51d1 or 123.
force		(Optional) Keyword used to allow LUN-mapping of the same storage array control LUNs in multiple targets.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines The **scsirouter target lun wwpn lun** command specifies a logical target name and LUN number combination to be mapped to a physical WWPN and LUN combination in storage.

**Tips**

WWPN address notation is represented by 16 hex digits. The digits may be separated by colons. When entering WWPN addresses, colons can be omitted or placed anywhere in the address notation as long as they do not leave one character without a partner character. The entry should be zero-filled from the most significant (the left-most) character position.

The following examples are *correct*:

- 0000:0000:1234:5678
- 0A0F2860:02111750
- 0A0F286002111750

The following examples are *incorrect*:

- 1:234:567:8:91:23:FF:6
- 12:34:56

The secondary WWPN and LUN combination is optional. The secondary combination is mapped to the logical target name and LUN combination as an alternate, if the primary WWPN and LUN combination is not available.

When you map a target using WWPN and the target needs to be accessed in a high availability cluster, you must specify both the primary WWPN (the WWPN of the storage resource as known to the first storage router in the cluster) and the secondary WWPN (the WWPN of the storage resource as known to the second storage router in the cluster). The secondary WWPN value may need to be retrieved by issuing the appropriate commands (such as the **show devices** command) from the second node in the cluster, or by temporarily attaching the secondary port of the storage device to the first storage router.

When a target is added, it is by default enabled. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts. Use the **scsirouter target accesslist** command to enable access to this storage target for selected IP hosts.

See [Chapter 6, “Configuring SCSI Routing,”](#) for more information about configuring SCSI routing instances on the SN 5428-2 Storage Router.

**Note**

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from [Cisco.com](#).

Use the **force** keyword to allow mapping of the same storage array control LUN in multiple targets. Do not use the **force** keyword to LUN-map the same data LUN in multiple targets. LUN-mapping of the same LUN in multiple targets is advised for a control LUN on a storage controller only.

Examples

The following example maps a logical target and LUN combination for SCSI router instance *lab3*. The logical target and LUN combination, *webserver7* LUN 7, is mapped to the primary WWPN and LUN combination, *2200002037191505* LUN 0.

```
[SN5428-2A]# scsirouter lab3 target webserver7 lun 7 wwpn 2200002037191505 lun 0
```

The following example maps a logical target and LUN combination to a primary and secondary WWPN. You may need to obtain the secondary WWPN from the storage router to which the secondary port of the device is attached, or temporarily attach the storage device's secondary port to the storage router being configured.

```
[SN5428-2A]# scsirouter lab4 target webserver8 lun 0 wwpn 2200002037c6756d lun 0 wwpn 2100002037c6747f lun 0
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
accesslist chap-username	Add CHAP user name entries to an access list.
accesslist iscsi-name	Add iSCSI Name entries to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
save scsirouter	Save configuration information for the named SCSI routing instance.
scsirouter	Create a SCSI routing instance.
scsirouter enable	Stop or start the named SCSI routing instance.
scsirouter primary	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
scsirouter target enable	Allow or disallow connections and logins for the named target.
setup scsi	Run the wizard to configure a SCSI routing instance.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter target maxcmdqueuedepth

To specify the maximum number of commands allowed at any given time from each iSCSI session to the specified target, use the **scsirouter target maxcmdqueuedepth** command.

scsirouter *name* **target** {*all* | *name*} **maxcmdqueuedepth** *nn*

Syntax Description

<i>name</i>	Name of the SCSI routing instance.
target all	Specify the maximum number of command for all targets.
target <i>name</i>	The name of the storage target.
<i>nn</i>	The maximum number of commands allowed from each iSCSI session. If the value is set to zero, the feature is disabled.

Defaults

This feature is disabled; **maxcmdqueuedepth** is set to zero.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced.

Usage Guidelines

When this value is configured, all current and future iSCSI sessions to the specified target will enforce the maximum command queue depth. To disable this feature, and allow an unlimited number of commands to the target from each iSCSI session, set the **maxcmdqueuedepth** to zero. This is the default setting.

Use the **show scsirouter** command with the **bootconfig** or **runningconfig** keyword to display the current maximum command queue depth value.



Note

Normal limitations, based on the available command buffer space, are always enforced. Setting the maximum command queue depth does not override these normal limitations.

Examples

The following example sets the maximum command queue depth to 20, for all targets associated with the SCSI routing instance named *foo*.

```
[SN5428-2A]# scsirouter foo target all maxcmdqueuedepth 20
```

The following example disables the maximum command queue depth, allowing an unlimited number of commands to the target named *webservices2*, associated with the SCSI routing instance named *foo*.

```
[SN5428-2A]# scsirouter foo target webservices2 maxcmdqueuedepth 0
```


Related Commands	Command	Description
	delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
	restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	scsirouter target enable	Allow or disallow connections and logins for the named target.
	show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter target profile

To disable the use of an initial iSCSI Ready-to-Transfer (R2T) on connections coming to this target, use the **scsirouter target profile** command.

scsirouter *name* **target** *name* **profile** {**high** | **low**}

Syntax Description

<i>name</i>	Name of the SCSI routing instance to which you are adding the target profile.
target <i>name</i>	The name of the storage target.
high	Disable the use of R2T for the specified target. This allows a host that opens a connection to the specified target to start sending data of a certain length as if it had received an initial R2T.
low	Enable the use of R2T for the specified target. This prevents a host that opens a connection to the specified target from sending any data packets to the target until the target has sent the host an R2T message. This adds latency to data transfer activities to this target.

Defaults

All targets are configured as high profile targets.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The SN 5428-2 Storage Router supports up to 16 concurrent connections that do not use an initial R2T. If there are 16 existing connections to targets configured as high profile, the 17th connection will be handled as though the target were defined as low profile, causing the connection performance to be a bit slower.

By default, all targets are defined as high profile targets to provide the best performance. Use the **scsirouter target profile** command to configure targets that do not require the additional performance as low profile targets.

Examples

The following example configures the target *labserver8* for SCSI routing instance *lab4* as a low profile target. Any host opening a connection to the *labserver8* target cannot send any data to the target until the target sends the host an R2T.

```
[SN5428-2A]# scsirouter lab4 target labserver8 profile low
```


Related Commands	Command	Description
	delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
	restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	scsirouter target enable	Allow or disallow connections and logins for the named target.
	show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter target wwpn

To map a logical target to a primary (and, optionally, a secondary) storage address specified by World Wide Port Names (WWPNs), use the **scsirouter target wwpn** command. The **scsirouter target wwpn** command is a target-only method of mapping a logical target specified by WWPNs.

scsirouter name target name wwpn xxxxxxxxxxxxxxxx [wwpn xxxxxxxxxxxxxxxx]

Syntax Description	name	Name of the SCSI routing instance to which you are adding the storage target.
	target name	A user-specified name of the logical target. Enter a maximum of 31 characters or a valid iSCSI Name. There is a maximum of 100 targets per storage router or per high availability cluster.
	wwpn xxxxxxxxxxxxxxxx	Specify a WWPN for the primary storage address. In a high availability cluster, this is the WWPN for the storage resource as known to the first storage router in the cluster.
	wwpn xxxxxxxxxxxxxxxx	(Optional) Specify a WWPN for the secondary storage address, used as an alternate for mapping if the primary is not available. In a high availability cluster, this is the WWPN for the storage resource as known to the second storage router in the cluster.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines The **scsirouter target wwpn** command requires only a logical target name to be mapped to a physical target address—no LUNS are specified. However, all LUNs that are part of the physical target address are discovered and made apparent as LUNs belonging to the logical target.



Tips

WWPN address notation is represented by 16 hex digits. The digits may be separated by colons. When entering WWPN addresses, colons can be omitted or placed anywhere in the address notation as long as they do not leave one character without a partner character. The entry should be zero-filled from the most significant (the left-most) character position.

The following examples are *correct*:

- 0000:0000:1234:5678
- 0A0F2860:02111750
- 0A0F286002111750

The following examples are *incorrect*:

- 1:234:567:8:91:23:FF:6
- 12:34:56

When you map a target using WWPN and the target needs to be accessed in a high availability cluster, you must specify both the primary WWPN (the WWPN of the storage resource as known to the first storage router in the cluster) and the secondary WWPN (the WWPN of the storage resource as known to the second storage router in the cluster). The secondary WWPN value may need to be retrieved by issuing the appropriate commands (such as the **show devices** command) from the second node in the cluster, or by temporarily attaching the secondary port of the storage device to the first storage router.

When a target is added, it is by default enabled. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts. Use the **scsirouter target accesslist** command to enable access to this storage target for selected IP hosts.

See [Chapter 6, “Configuring SCSI Routing,”](#) for more information about configuring SCSI routing instances on the SN 5428-2 Storage Router.



Note

When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

Examples

The following example maps a logical target for SCSI router instance *lab4*. The logical target *webserver1* is mapped to the primary WWPN, 22:00:00:20:37:19:15:05.

```
[SN5428-2A]# scsirouter lab4 target webserver1 wwpn 22:00:00:20:37:19:15:05
```

The following example maps a logical target to a primary and secondary WWPN. You may need to obtain the secondary WWPN from the storage router to which the secondary port of the device is attached, or temporarily attach the storage device’s secondary port to the storage router being configured.

```
[SN5428-2A]# scsirouter lab5 target webserver9 wwpn 2200002037c6756d wwpn 2100002037c6747f
```


Related Commands	Command	Description
	accesslist	Create an access list entity.
	accesslist A.B.C.D/bits	Add IP addresses to an access list.
	accesslist chap-username	Add CHAP user name entries to an access list.
	accesslist iscsi-name	Add iSCSI Name entries to an access list.
	delete accesslist	Delete a specific access list entry or an entire access list.
	delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
	restore accesslist	Restore the named access list or all access lists from the named configuration file.
	restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
	save accesslist	Save configuration data for the named access list or all access lists.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	scsirouter	Create a SCSI routing instance.
	scsirouter enable	Stop or start the named SCSI routing instance.
	scsirouter primary	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
	scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
	scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
	setup scsi	Run the wizard to configure a SCSI routing instance.
	show accesslist	Display the contents of the named access list or all access lists.
	show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter username

To assign a user name to a SCSI routing instance for iSCSI authentication purposes, use the **scsirouter username** command.

```
scsirouter name username {user-name | none}
```

Syntax Description	<i>name</i>	The name of the SCSI routing instance.
	<i>user-name</i>	A valid user name. Enter a maximum of 63 characters
	none	Keyword, removing any existing iSCSI user name assigned to the named SCSI routing instance.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Use this command to assign a user name to the SCSI routing instance for two-way iSCSI authentication. Two way iSCSI authentication allows authentication of the IP host and also allows the IP host, acting as an iSCSI initiator, to require authentication of the SCSI routing instance, acting as an iSCSI target. The user name and password assigned to the SCSI routing instance are used by the IP host for iSCSI authentication purposes.

iSCSI authentication must be enabled for the named SCSI routing instance. If iSCSI authentication is not enabled, the user name and password assigned to the SCSI routing instance will not be used.

Examples

The following example enables iSCSI authentication, using the default authentication list, for the SCSI routing instance named *lab3* and assigns a user name of *lab3-admin* and a password of *testing* to the instance for two-way authentication:

```
[SN5428-2A]# scsirouter lab3 authentication default
* [SN5428-2A]# scsirouter lab3 username lab3-admin
* [SN5428-2A]# scsirouter lab3 password testing
```


Related Commands	Command	Description
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	scsirouter password	Assign a password to a SCSI routing instance for iSCSI authentication purposes.
	show scsirouter	Display configuration and operational information for the named SCSI routing instance.

session-timeout

To set the number of minutes a Telnet or SSH management session (or an Administrator mode session via the EIA/TIA-232 console connection) to the SN 5428-2 Storage Router can be inactive before the session times out, use the **session timeout** command. To prevent management sessions from timing out, use the **no** form of this command.

session-timeout *nn*

no session-timeout

Syntax Description	<i>nn</i>	The number of minutes the management session can be inactive before it is terminated. By default, management sessions do not timeout.
--------------------	-----------	---

Defaults	There is no timeout for management sessions. This has the same effect as the following command: session-timeout 0	
----------	---	--

Command Modes	Administrator.	
---------------	----------------	--

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	<p>Use this command to configure the number of minutes a Telnet or SSH management session (or an Administrator mode session via the console) can be inactive before it is terminated. By default, management sessions do not time out.</p> <p>When an Administrator mode session via the console times out, the console returns automatically to Monitor mode. If passwords are enabled on the console, the password prompt displays.</p> <p>A change in the session timeout value is effective at the next time-check interval, and will affect all currently logged in management sessions as well as future sessions, until the storage router is restarted.</p> <p>Use the show system command to display the current time out value for management sessions.</p>
------------------	--

Examples	<p>The following example allows management sessions to be inactive for 15 minutes before being terminated.</p> <pre>[SN5428-2A]# session-timeout 15</pre> <p>The following example disables automatic termination of inactive management sessions:</p> <pre>[SN5428-2A]# no session-timeout</pre>
----------	---

Related Commands	Command	Description
	show sessions	Display information about active console, Telnet, SSH or GUI sessions to the storage router.
	show system	Display selected system information.

setup

To configure the SN 5428-2 Storage Router using the setup configuration wizard, use the **setup** command. The Setup configuration wizard runs the Management Interface, Date and Time, Network Management, Management Access, and SCSI routing (if applicable) individual wizards in sequence.

setup

Syntax Description

This command has no arguments or keywords.

Defaults

For multiple choice questions, the system presents the choices enclosed in brackets, []. Each multiple choice question has a default answer that is selected when you press Enter or Return. The default is shown in parentheses, (). For example:

```
Enable High Availability? [yes/no (no)]
```

For configuration variables, the current value saved in the system is presented in brackets. For example:

```
Network mask ? [255.255.255.0]
```

If the configuration variable does not have a value, the system will present a set of “empty” brackets, [(empty)], or a template that provides the required format of the value. For example:

```
SN5428-2 system name? [(empty)]
```

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Initial system configuration and subsequent reconfiguration can be performed via interactive configuration wizards through the console interface (or via Telnet or SSH once the management interface has been configured). The configuration wizards prompt you for the necessary information to accomplish the specific configuration task and may invoke multiple commands to complete their functions.

The CLI provides the following configuration wizards:

- Setup—runs the Management Interface, Date and Time, Network Management, Management Access, and SCSI routing (if applicable) individual wizards in sequence.
- Management Interface—configures the management interface with a system name, IP address, and optional DNS server information.
- Date and Time—configures the time zone, use (or non-use) of daylight savings time, and the NTP server address (if one is present) or the current date and time.
- Network Management—configures the use of Telnet, web-based GUI, and SNMP for managing the storage router over the network.

- Management Access—configures passwords for monitoring and configuring the storage router.
- SCSI Routing—configures a SCSI routing instance. The wizard is only available when the storage router is deployed for SCSI routing; it is not available if the storage router is deployed for transparent SCSI routing.
- FCIP—configures FCIP instances. The wizard is only available when the storage router is deployed for FCIP; it is not available if the storage router is deployed for SCSI routing or transparent SCSI routing.

If the storage router is deployed for SCSI routing, the CLI also provides a Cluster wizard, which configures the storage router to participate in a high availability cluster. Because the initial configuration script configures the high availability environment, the Setup configuration wizard does not include the Cluster wizard. However, the Cluster wizard, using the [setup cluster](#) command, can be run after initial system configuration to change the configuration mode from standalone to clustered, to change membership from one cluster to another, or to resign from a cluster and run as a standalone storage router. See [Chapter 2, “First-Time Configuration,”](#) for more information about initial system configuration.

During configuration with the Setup configuration wizard, operational changes take place and are applied to the currently running system. For example, after the Network Management wizard completes, SNMP network management will be configured for the storage router. However, these changes are not saved to the system’s bootable configuration until the end of the entire Setup configuration wizard. To quit the setup configuration wizard without saving changes, press **Ctrl-C** at any time before the end of the wizard, and then reboot the storage router to restore previous values.

**Note**

Some changes may be retained after a reboot. Be sure to review the values provided in the prompts that display if you rerun the setup configuration wizard or run each individual wizard.

After entering the Setup configuration wizard, several informational messages display, including the following prompt:

```
User level for setup? [novice/expert (expert)]
```

- Enter **novice** to continue with the configuration process. Explanatory text displays before each prompt in the wizard.
- Enter **expert** to continue with the configuration process, suppressing all explanatory text. If you are an experienced user familiar with the setup configuration wizard, you may prefer this option.

At the end of the Setup configuration wizard, the following prompt displays:

```
Done with setup.
```

**Note**

Only one setup wizard can be active at any given time. Multiple users cannot run multiple setup wizards concurrently.

Examples

The following shows the initial explanatory text for the **setup** command:

```
[SN5428-2_A]# setup
```

You are about to set up the SN5428-2. Running this wizard will modify the configuration of this system.

During setup, operational changes will take place. However, these changes are not saved until the end of the script. To quit the setup wizard without saving changes, ** hit CTRL-C at any time **. Reboot to restore previous values.

For multiple choice questions, the system will present the choices enclosed in brackets []. Each multiple choice question has a default answer that is selected when you press return.

Example: [yes/no (no)].

Choices are yes and no. No is the default answer.

For configuration variables, the current value saved in the system is presented in brackets [varname]. If the configuration variable does not have a value, the system will present a set of brackets [(empty)] or a template that provides the expected format of the value.

Example: [mySN5428-2] configuration variable has a value

Example: [(empty)] configuration variable does not have a value, no template

Example: [A.B.C.D] template for an IP address.

User level for setup? [novice/expert (expert)]

Related Commands

Command	Description
clear conf	Return most configuration settings to factory defaults.
setup access	Run the wizard to configure Monitor mode and Administrator mode passwords.
setup cluster	Change the configuration of the high availability environment.
setup fcip	Run the wizard to manually configure FCIP instances.
setup iscsi-port	Run the wizard to manually configure the port used for iSCSI traffic.
setup mgmt	Run the wizard to configure the management interface.
setup netmgmt	Run the wizard to configure network management.
setup scsi	Run the wizard to configure a SCSI routing instance.
setup time	Run the wizard to configure the system date and time.

setup access

To configure passwords for monitoring and administering the SN 5428-2 Storage Router, use the **setup access** configuration wizard. The wizard prompts you to enter and confirm new passwords.

setup access [*parameter1 parameter2...*]

Syntax Description

<i>parameter1 parameter2 ...</i>	(Optional) Enter each parameter that the wizard prompts for. All parameters must be passed. If a parameter includes an embedded space, enclose the parameter in quotation marks.
----------------------------------	--

Defaults

The factory default password for both Administrator mode and Monitor mode is *cisco*.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The wizard prompts you to enter (and confirm by re-entering) the new Monitor password, which allows view-only access to the storage router. It also prompts you to enter (and confirm by re-entering) the new Administrator password, which allows changes to be made to the storage router configuration. Passwords are cluster configuration elements. In a high availability (HA) cluster, the **setup access** wizard can only be run from the storage router that is currently performing password management functions.

Only one setup wizard can be active at any given time. Multiple users cannot run multiple setup wizards concurrently.

Use the optional *parameter* arguments to run the **setup access** wizard from a command script. All parameters required by the wizard must be included. The **setup access** wizard will not complete unless all parameters are passed.



Note

If too many parameters are passed, the **setup access** wizard will ignore the extra parameters and may complete. If a parameter is not in the correct format or is otherwise invalid, the next parameter is used to attempt to fulfill the prompt. In either case, unexpected results could occur. Always check the output from a **setup access** command when using the *parameter* arguments.

Examples

The following example sets the Monitor mode and Administrator mode passwords for the storage router, but does not apply them to the console interface. Administrator contact information is also configured. Passwords display as asterisks when entered.

```
[SN5428-2_PR]# setup access
```

```
#####
## Management Access Setup ##
#####
```

The SN5428-2 CLI and GUI are protected by two passwords. The initial password entered when logging in allows the user to monitor the SN5428-2, but does not allow changes. The "admin" password allows the user to make configuration changes.

```
Enter the current "monitor" password:*****
```

```
** Password Rules **
```

A password can contain any combination of numbers and letters, but should not be something familiar to you and easy to guess.

```
Enter the new "monitor" password: *****
```

```
Enter the new "monitor" password again: *****
```

```
Enter the current "admin" password: *****
```

```
Enter the new "admin" password: *****
```

```
Enter the new "admin" password again: *****
```

The new passwords will apply to all telnet and web-based GUI sessions. They will also be applied to the console. If the SN5428-2 console is in a physically secure location, console passwords are not recommended since they can be lost or forgotten. If the SN5428-2 is deployed in a less secure environment, the passwords should be applied. If passwords are subsequently lost, visit http://www.cisco.com/public/Support_root.shtml for information on recovery.

```
Apply passwords to console ? [yes/no (no)] no
```

The administrative contact is the person or group responsible for configuration and management of the SN5428-2. The system will store a name, e-mail address, phone number, and pager number for the system administrator. Management applications can retrieve this information and provide it to a support person or directly use it to e-mail or page the administrator.

```
Input Administrator Info? [yes/no (yes)] yes
```

```
Administrator name? [(empty) ] Pat Hurley
```

```
Phone? [(empty) ] 123.456.7890
```

```
Pager number? [(empty)] 12.456.3444 pin 2234
```

```
Email? [(empty)] hurley@abc123z.com
```

```
Done with setup.
```


Related Commands	Command	Description
	clear conf	Return most configuration settings to factory defaults.
	setup	Run the setup configuration wizard.
	setup cluster	Change the configuration of the high availability environment.
	setup fcip	Run the wizard to manually configure FCIP instances.
	setup iscsi-port	Run the wizard to manually configure the port used for iSCSI traffic.
	setup mgmt	Run the wizard to configure the management interface.
	setup netmgmt	Run the wizard to configure network management.
	setup scsi	Run the wizard to configure a SCSI routing instance.
	setup time	Run the wizard to configure the system date and time.

setup cluster

To configure the high availability (HA) environment for the SN 5428-2 Storage Router, to add the storage router to a cluster, or to remove it from an existing cluster, use the **setup cluster** configuration wizard. The wizard prompts you to select the appropriate HA configuration mode, enter a cluster name and (if necessary) an HA interface IP address and subnet mask.

setup cluster [*parameter1 parameter2...*]

Syntax Description	<i>parameter1 parameter2 ...</i> (Optional) Enter each parameter that the wizard prompts for. All parameters must be passed. If a parameter includes an embedded space, enclose the parameter in quotation marks.
--------------------	---

Defaults	<p>Defaults or current values are shown in parentheses within the allowable response brackets. In the following example, the allowable responses are <i>retain</i> and <i>delete</i>, and the default is <i>delete</i>.</p> <pre>Retain or delete applications ? [retain/delete (delete)]</pre>
----------	---

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	<p>The HA features of the SN 5428-2 Storage Router are designed around a cluster of systems that back each other up in case of failure. A cluster consists of two identically configured SN 5428-2s (or one SN 5428 and one SN 5428-2) that continually exchange HA information over their HA and management interfaces.</p> <p>Clusters are defined by name. The setup cluster command prompts you for the appropriate HA configuration mode and the cluster name.</p> <ul style="list-style-type: none"> Use the standalone keyword to identify the storage router as not participating in a cluster. A standalone storage router does not require the management or HA interfaces to be available in order to complete the system configuration. The MGMT and HA ports do not need to be cabled. Use the clustered keyword to identify the storage router as participating in a cluster. A clustered SN 5428-2 requires the management and HA interfaces to be available in order to complete the system configuration. The MGMT and HA ports must be correctly cabled. <p>The command also prompts you to either retain the SCSI routing instance configurations for this storage router, merging them with others in the cluster, or to delete the existing SCSI routing instance configuration data and replace it with cluster data. Retained SCSI routing instance configuration data is replicated to other storage routers in the cluster. When joining an existing cluster, access list information and other cluster configuration elements, including VLAN, AAA and password settings, are always deleted and replaced by the cluster's access lists and other cluster configuration elements.</p>
------------------	--

**Caution**

Retaining SCSI routing instance configuration data could provide unexpected results.

Changing the cluster name, thereby joining another cluster, has the following effects on its existing configurations and operations:

- All SCSI routing instances are failed over to another member in the original cluster.
- All applications are stopped.
- The cluster name is changed.
- If you choose to retain data, any unsaved cluster configuration information is saved.
- The system reboots. Configuration information is exchanged and the storage router learns AAA, access list, password, SCSI routing instance and VLAN configuration information from the cluster. All of the original SCSI routing instances appears in the new cluster, unless you chose to delete rather than retain data.
- Access lists that existed on the storage router prior to joining the new cluster are always deleted. To preserve an existing access list and make it available to the new cluster, you must save the access list to a configuration file before issuing the **setup cluster** command. Make the saved configuration file available to the storage router currently performing access list maintenance functions for the cluster (via the **copy** command), and then restore the saved access list to the new cluster from that configuration file. See [Chapter 10, “Configuring a High Availability Cluster,”](#) for more information about configuring the storage router to participate in a cluster.
- For cases where the names of SCSI routing instances are duplicated within the new cluster (meaning instances of the same name are already running in the new cluster), configuration data from the old cluster is deleted in favor of what is currently running in the new cluster.

Only one setup wizard can be active at any given time. Multiple users cannot run multiple setup wizards concurrently.

Use the optional *parameter* arguments to run the **setup cluster** wizard from a command script. All parameters required by the wizard must be included. The **setup cluster** wizard will not complete unless all parameters are passed.

**Note**

If too many parameters are passed, the **setup cluster** wizard will ignore the extra parameters and may complete. If a parameter is not in the correct format or is otherwise invalid, the next parameter is used to attempt to fulfill the prompt. In either case, unexpected results could occur. Always check the output from a **setup cluster** command when using the *parameter* arguments.

Examples

The following shows example output and input for the **setup cluster** command:

```
[SN5428-2_PR]# setup cluster
```

```
The system has the ability to run in a standalone or clustered state.
By default, the system will run in a clustered state and communicate
with other SN5428-2s in the same cluster. If a single SN5428-2 is deployed
and you don't intend to add a second SN5428-2 to provide high availability
features in a clustered configuration, you should configure the SN5428-2 in
standalone mode. Enter CTRL-C at any prompt to cancel changes and return
to the command prompt.
```

```
HA configuration? [standalone/clustered (standalone)] clustered
```


If you select HA configuration mode *clustered*, the wizard prompts you to enter an HA IP address:

To determine the health of other SN5428-2s in a cluster, the SN5428-2 must send occasional heartbeat packets on at least two interfaces (in case one interface has problems). By default, the interfaces used are the 10/100 management interface (already set up) and the 10/100 HA interface. Please select an IP address and network mask for the HA interface.

```
HA Interface IP address? [10.1.40.230/24]
```

After selecting the HA configuration mode, and optionally setting the HA IP address, the wizard prompts you to enter a cluster name:

When you change the cluster that the SN5428-2 belongs to, you need to decide if you want the scsirouter instances running on the SN5428-2 to be deleted or if you want them to be retained and merged with the new cluster.

```
Change cluster to ? [Cluster1]
```

For a change from standalone to clustered:

If you retain the configuration, there may be conflicts when the scsirouter instances are replicated between this SN5428-2 and others in the new cluster.

For a change from clustered to standalone:

You can retain the configuration without causing any scsirouter instance conflicts for this SN5428-2 since it will be the only member of the new cluster.

```
Retain or delete scsirouter instances ? [retain/delete (delete)] retain
```

If you choose to retain the existing SCSI routing instance configurations, an additional warning displays:

```
#####
Please confirm that you want to retain the configuration.
#####
```

```
All configuration settings will be saved.
The system will REBOOT if you answer "yes"
** Enter CTRL-C to cancel. **
```

```
Are you sure you want to retain the configuration ? [must type "yes"] yes
```

If you choose to delete your existing configuration, this warning displays:

```
Retain or delete applications ? [retain/delete (delete)] delete
```

```
#####
Please confirm that you want to delete the configuration.
#####
```

```
Cluster configuration settings will be saved.
The system will REBOOT if you answer "yes"
** Enter CTRL-C to cancel and abort the cluster change. **
```

```
Are you sure you want to delete the configuration ? [must type "yes"] yes
```

After confirming your selection, the storage router automatically reboots.

Related Commands	Command	Description
	clear conf	Return most configuration settings to factory defaults.
	setup	Run the setup configuration wizard.
	setup access	Run the wizard to configure Monitor mode and Administrator mode passwords.
	setup fcip	Run the wizard to manually configure FCIP instances.
	setup iscsi-port	Run the wizard to manually configure the port used for iSCSI traffic.
	setup mgmt	Run the wizard to configure the management interface.
	setup netmgmt	Run the wizard to configure network management.
	setup scsi	Run the wizard to configure a SCSI routing instance.
	setup time	Run the wizard to configure the system date and time.

setup fcip

To configure an FCIP instance, use the **setup fcip** configuration wizard. The wizard prompts you to choose the name of the FCIP instance and specify the Gigabit Ethernet IP address and network mask. Then the wizard prompts you to enter the peer IP address and the connection protocol type. More extensive configuration of FCIP instances can be performed via the CLI or the web-based GUI.

setup fcip [*parameter1 parameter2...*]

Syntax Description	<i>parameter1 parameter2 ...</i> (Optional) Enter each parameter that the wizard prompts for. All parameters must be passed. If a parameter includes an embedded space, enclose the parameter in quotation marks.
--------------------	---

Defaults	<p>Defaults or current values are shown in parentheses within the allowable response brackets. In the following example, the current default FCIP instance name is <i>fcip1</i>.</p> <pre>Create which FCIP instance ? [fcip1/fcip2 (fcip1)]</pre>
----------	--

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.3.1	This command was introduced.

Usage Guidelines	<p>The setup fcip command can only be run when at least one FCIP instance is not currently configured on the storage router; if both FCIP instances are configured, you cannot run the setup fcip wizard. Only one setup wizard can be active at any given time. Multiple users cannot run multiple setup wizards concurrently.</p> <p>Use the optional <i>parameter</i> arguments to run the setup fcip wizard from a command script. All parameters required by the wizard must be included. The setup fcip wizard will not complete unless all parameters are passed.</p>
------------------	--



Note

If too many parameters are passed, the **setup fcip** wizard will ignore the extra parameters and may complete. If a parameter is not in the correct format or is otherwise invalid, the next parameter is used to attempt to fulfill the prompt. In either case, unexpected results could occur. Always check the output from a **setup fcip** command when using the *parameter* arguments.

Examples

The following shows example output and input for the **setup scsi** command:

```
[techpubs4]# setup fcip
```

In order to correctly configure this FCIP instance, be sure you know the configuration of the remote FCIP instance. You will need to know the IP address and the communication protocol of the remote FCIP instance. In addition, you will need to ensure that the Fibre Channel domain ID you assign is different than the Fibre Channel domain ID assigned to the remote SN 5428-2-K9.

The system enables you to create two FCIP instances. Each instance uses a different Fibre Channel interface and gigabit Ethernet interface.

```
Create which FCIP instance ? [fcip1/fcip2 (fcip1)] fcip2
```

Please specify an IP address and netmask for the gigabit Ethernet interface.

```
IP address? [A.B.C.D/nn] 10.1.0.16/24
```

If both gigabit Ethernet interfaces are cabled to the same network, you can configure the FCIP instance to failover to the secondary interface in case of a failure on the primary interface.

```
Configure secondary interface for the FCIP instance? [yes/no (no)] no
```

Please enter the IP address of the remote FCIP instance to which you wish to connect.

```
IP address of remote FCIP instance? [A.B.C.D] 10.1.0.47
```

Choose how you want the FCIP instance to communicate with the remote FCIP instance. If the remote FCIP instance is configured to use raw IP, select raw as the protocol. If the remote FCIP instance is configured as a TCP server, select client. If the remote FCIP instance is configured as a TCP client, select server.

```
Use which protocol? [raw/client/server] raw
```

If this is the first FCIP instance to be configured on the storage router, you will be prompted to specify a Fibre Channel domain ID:

Please specify a domain ID for use by this FCIP instance. This domain ID must be unique. It can not be assigned to any switch in the Fibre Channel fabric that this switch is connected to or assigned to any switch in the remote Fibre Channel network.

```
Domain ID for the Fibre Channel switch? [1 - 127] 80
```

```
set Domain ID on Fibre Channel interfaces to 80
```

```
Mar 14 15:08:48: %FC-5-FCIP09: fcip2 has been started
```

```
FCIP, fcip2, created
```

```
Mar 14 15:08:48: %UI-5-FAFD2: Added FCIP device fci2
```

```
Mar 14 15:08:48: %UI-5-NMAOOI: Address 10.1.0.16/24 is now operational on interface ge1
```

```
Mar 14 15:08:48: %UI-5-FAFNI: Added FCIP network interface ge2, 10.1.0.16/255.255.0
```

```
FCIP-2: addPeer raw 10.1.0.47
```

```
Mar 14 15:08:48: %UI-5-FAFD: Added FCIP destination dest2 (raw, 10.1.50.50)
```

```
Configuration complete.
```

FCIP instance fcip2 is now configured.


Done with setup.

Related Commands	Command	Description
	clear conf	Return most configuration settings to factory defaults.
	setup	Run the setup configuration wizard.
	setup access	Run the wizard to configure Monitor mode and Administrator mode passwords.
	setup cluster	Change the configuration of the high availability environment.
	setup iscsi-port	Run the wizard to manually configure the port used for iSCSI traffic.
	setup mgmt	Run the wizard to configure the management interface.
	setup netmgmt	Run the wizard to configure network management.
	setup scsi	Run the wizard to configure a SCSI routing instance.
	setup time	Run the wizard to configure the system date and time.

setup iscsi-port

To change the default listening port used for iSCSI traffic, use the **setup iscsi-port** wizard.

setup iscsi-port [*parameter1 parameter2...*]

Syntax Description	<i>parameter1 parameter2 ...</i> (Optional) Enter each parameter that the wizard prompts for. All parameters must be passed. If a parameter includes an embedded space, enclose the parameter in quotation marks.				
Defaults	The default listening port used for iSCSI traffic is 3260. This is the port number assigned by IANA.				
Command Modes	Administrator.				
Command History	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>3.2.1</td><td>This command was introduced.</td></tr> </table>	Release	Modification	3.2.1	This command was introduced.
Release	Modification				
3.2.1	This command was introduced.				
Usage Guidelines	<p>If you change the listening port used for iSCSI traffic on the storage router, you must make corresponding changes to the IP hosts sending iSCSI traffic to the storage router. For example, on a UNIX system, you must update the <code>/etc/services</code> file. After selecting a new port for iSCSI traffic, the storage router automatically reboots.</p> <p>Only one setup wizard can be active at any given time. Multiple users cannot run multiple setup wizards concurrently.</p> <p>Use the optional <i>parameter</i> arguments to run the setup iscsi-port wizard from a command script. All parameters required by the wizard must be included. The setup iscsi-port wizard will not complete unless all parameters are passed.</p>				
 Note	If too many parameters are passed, the setup iscsi-port wizard will ignore the extra parameters and may complete. If a parameter is not in the correct format or is otherwise invalid, the next parameter is used to attempt to fulfill the prompt. In either case, unexpected results could occur. Always check the output from a setup iscsi-port command when using the <i>parameter</i> arguments.				

Examples

The following shows example output and input for the **show iscsi-port** command:

```
[SN5428-2A]# setup iscsi-port

#####
##  iSCSI port Setup Wizard  ##
#####
If you change the iSCSI port number, the system will reboot itself
for the change to take effect. This will cause all scsirouters to
be stopped.
** Enter CTRL-C to cancel. **
```



```

Do you want to change the iSCSI port number?[yes/no (no)] yes

#####
## Changing iSCSI port ##
#####
Now, you will need to enter a new iSCSI port number. The new port
will be used as the iSCSI server listen port. Make sure the new
port is not used by other applications in your network environment.

New port number ? [nn] 5003

#####
## Please confirm that you want to change iSCSI port ##
#####

iSCSI port configuration settings will be saved.
The system will REBOOT if you answer "yes".
** Enter CTRL-C to cancel. **

Proceed to change the iSCSI port?[yes/no (no)] yes

```

After confirming your intentions, the storage router automatically reboots.

Related Commands

Command	Description
clear conf	Return most configuration settings to factory defaults.
setup	Run the setup configuration wizard.
setup access	Run the wizard to configure Monitor mode and Administrator mode passwords.
setup fcip	Run the wizard to manually configure FCIP instances.
setup cluster	Change the configuration of the high availability environment.
setup mgmt	Run the wizard to configure the management interface.
setup netmgmt	Run the wizard to configure network management.
setup scsi	Run the wizard to configure a SCSI routing instance.
setup time	Run the wizard to configure the system date and time.

setup mgmt

To configure the SN 5428-2 Storage Router management interface, use the **setup mgmt** configuration wizard. The wizard prompts you to enter the system name, management interface IP address and subnet mask, optional default gateway and DNS information.

setup mgmt [*parameter1 parameter2...*]

Syntax Description

<i>parameter1 parameter2 ...</i>	(Optional) Enter each parameter that the wizard prompts for. All parameters must be passed. If a parameter includes an embedded space, enclose the parameter in quotation marks.
----------------------------------	--

Defaults

Defaults or current values are shown in parentheses within the allowable response brackets. In the following example, the current system name is *SN5428-2_Lab1*.

```
SN5428-2 system name? [SN5428-2_Lab1]
```

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The management interface must be configured before the Telnet interface or web-based GUI can be used for configuration or monitoring tasks. When the wizard is completed, the system displays notification that the management interface is operational.

Only one setup wizard can be active at any given time. Multiple users cannot run multiple setup wizards concurrently.

Use the optional *parameter* arguments to run the **setup mgmt** wizard from a command script. All parameters required by the wizard must be included. The **setup mgmt** wizard will not complete unless all parameters are passed.



Note

If too many parameters are passed, the **setup mgmt** wizard will ignore the extra parameters and may complete. If a parameter is not in the correct format or is otherwise invalid, the next parameter is used to attempt to fulfill the prompt. In either case, unexpected results could occur. Always check the output from a **setup mgmt** command when using the *parameter* arguments.

Examples

The following shows example output for the **setup mgmt** command:

```
[SN5428-2A]# setup mgmt

#####
## Management Interface Setup ##
#####

Please choose a name for the SN5428-2. This name is associated with the
SN5428-2 Management Interface IP address. If you wish to enable network
management on the SN5428-2, you should add the system name you provide
at this prompt and its IP address to a domain name server (nis, nis+, WINS).

SN5428-2 system name? [SN5428-2A]

The SN5428-2 may be managed using telnet, or a web-based GUI, or SNMP via the
10/100 Ethernet interface labeled "mgmt" on the front panel of the system. This
interface must be assigned an IP address.

Management Interface IP address? [10.1.12.122/24]

If the SN5428-2 is to be managed from a subnet other than the one to which it
is physically attached, a static route is required. The static route format
is "destination/netmask gateway".

Static route for Management Interface? [0.0.0.0/0 10.1.12.1]

If IP addresses are to be entered as host names via any of the SN5428-2
management interfaces, a Domain Name Server must be specified. A secondary
DNS may be specified for use if the primary DNS is not available.

Primary DNS Server? [A.B.C.D]

Secondary DNS Server? [A.B.C.D]

Setting up the management interface ... Done

The management port is now operational. It may be tested using ping
or telnet from a host on the network.

Done with setup.
```

Related Commands

Command	Description
clear conf	Return most configuration settings to factory defaults.
setup	Run the setup configuration wizard.
setup access	Run the wizard to configure Monitor mode and Administrator mode passwords.
setup cluster	Change the configuration of the high availability environment.
setup fcip	Run the wizard to manually configure FCIP instances.
setup iscsi-port	Run the wizard to manually configure the port used for iSCSI traffic.
setup netmgmt	Run the wizard to configure network management.
setup scsi	Run the wizard to configure a SCSI routing instance.
setup time	Run the wizard to configure the system date and time.

setup netmgmt

To enable network management via any or all of the available interfaces (Telnet, web-based GUI, or SNMP), use the **setup netmgmt** configuration wizard. The wizard prompts you to selectively enable the various interfaces and, if SNMP is enabled, will prompt you to enter the read and write community information, IP addresses for SNMP traps, and additional SNMP configuration information.

setup netmgmt [*parameter1 parameter2...*]

Syntax Description

parameter1 parameter2 ... (Optional) Enter each parameter that the wizard prompts for. All parameters must be passed. If a parameter includes an embedded space, enclose the parameter in quotation marks.

Defaults

Defaults or current values are shown in parentheses within the allowable response brackets. In the following example, the default name for the read community is *public*:

Read Community ? [public]

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

All network management interfaces are enabled by default, with SNMP “gets” via the public read community. Run this wizard to disable any of these interfaces, or to change the SNMP read community, configure the SNMP write community for SNMP “sets,” or add addresses for SNMP traps.

Only one setup wizard can be active at any given time. Multiple users cannot run multiple setup wizards concurrently.

Use the optional *parameter* arguments to run the **setup netmgmt** wizard from a command script. All parameters required by the wizard must be included. The **setup netmgmt** wizard will not complete unless all parameters are passed.



Note

If too many parameters are passed, the **setup netmgmt** wizard will ignore the extra parameters and may complete. If a parameter is not in the correct format or is otherwise invalid, the next parameter is used to attempt to fulfill the prompt. In either case, unexpected results could occur. Always check the output from a **setup netmgmt** command when using the *parameter* arguments.

Examples

The following shows example output and input for the **setup netmgmt** command:

```
[SN5428-2A]# setup netmgmt
#####
## Network Management Access Setup ##
#####
```

This wizard will enable you to configure access to telnet, the web-based GUI, and configure SNMP. By default, telnet and the web-based GUI are enabled. SNMP gets via the "public" community are also enabled via the 10/100 management interface. If you want to change these values or configure other SNMP features, please set up the network management.

Set up Network Management ? [yes/no (yes)] **yes**

Enable telnet on all interfaces? [yes/no (yes)] **yes**

Configure SNMP ? [yes/no (yes)] **yes**

If you select to configure SNMP, the wizard prompts you for the following information:

Read Community ? [public]

Write Community ? [private] **mynetmanagers**

First IP address for SNMP traps ? [A.B.C.D] **10.1.30.17**

Trap version for first IP address? [1/2 (1)]

Second IP address for SNMP traps ? [A.B.C.D] **10.1.30.18**

Trap version for second IP address? [1/2 (1)]

Send auth trap when requester specifies
incorrect community? [yes/no (no)] **yes**

Modify link up/down traps for one or more interfaces? [yes/no (yes)] **yes**

Send link up/down traps for MGMT interface? [yes/no (yes)] **yes**

Send link up/down traps for HA interface? [yes/no (yes)] **yes**

Send link up/down traps for GE interface? [yes/no (yes)] **no**

Send link up/down traps for fibre
channel interface? [yes/no (yes)] **yes**

The wizard ends by displaying the following information:

Network Management setup is complete.

By default, these methods of network management will work from any network which is not separated from the SN5428-2 by a firewall or other traffic-limiting device. To further specify security requirements, please use the normal configuration functions of the CLI or GUI after completing this wizard.

Done with setup.

Related Commands	Command	Description
	clear conf	Return most configuration settings to factory defaults.
	setup	Run the setup configuration wizard.
	setup access	Run the wizard to configure Monitor mode and Administrator mode passwords.
	setup cluster	Change the configuration of the high availability environment.
	setup fcip	Run the wizard to manually configure FCIP instances.
	setup iscsi-port	Run the wizard to manually configure the port used for iSCSI traffic.
	setup mgmt	Run the wizard to configure the management interface.
	setup scsi	Run the wizard to configure a SCSI routing instance.
	setup time	Run the wizard to configure the system date and time.

setup scsi

To configure a SCSI routing instance, use the **setup scsi** configuration wizard. The wizard prompts you to enter the name of the SCSI routing instance (maximum 32 characters) and to specify the IP address and Gigabit Ethernet interface for the SCSI routing instance. Then the wizard discovers all Fibre Channel devices connected to the SN 5428-2 Storage Router. More extensive configuration of SCSI routing instances can be performed via the CLI or the web-based GUI.

setup scsi [*parameter1 parameter2...*]

Syntax Description

parameter1 parameter2 ... (Optional) Enter each parameter that the wizard prompts for. All parameters must be passed. If a parameter includes an embedded space, enclose the parameter in quotation marks.

Defaults

Defaults or current values are shown in parentheses within the allowable response brackets. In the following example, the current default Gigabit Ethernet interface is *ge1*.

```
Scsirouter instance GE interface ? [ge1|ge2 (ge1)]
```

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

After the wizard finishes the discovery process, it displays a list of accessible storage resources. Targets can be explicitly added by using the web-based GUI or CLI commands.

The **setup scsi** command can only be run when no SCSI routing instance is currently configured on the storage router. Only one setup wizard can be active at any given time. Multiple users cannot run multiple setup wizards concurrently.

Use the optional *parameter* arguments to run the **setup scsi** wizard from a command script. All parameters required by the wizard must be included. The **setup scsi** wizard will not complete unless all parameters are passed.



Note

If too many parameters are passed, the **setup scsi** wizard will ignore the extra parameters and may complete. If a parameter is not in the correct format or is otherwise invalid, the next parameter is used to attempt to fulfill the prompt. In either case, unexpected results could occur. Always check the output from a **setup scsi** command when using the *parameter* arguments.

Examples

The following shows example output and input for the **setup scsi** command:

```
[SN5428-2A]# setup scsi
#####
##  scsirouter Setup ##
#####
This wizard will enable you to set up a scsirouter instance, but will not enable you to
specify a VLAN for the IP interface. If a VLAN is required for the scsirouter instance,
please use CLI commands to configure the scsirouter.
Do you want to configure a scsirouter instance ? [yes/no (no)] yes

scsirouter instance name ? [(empty)] foo

The scsirouter instance communicates with IP hosts via the Gigabit Ethernet interface. To
enable communication, you need to assign an IP address and network mask to the scsirouter
instance for it to use on the Ethernet interface.

IP Address ? [A.B.C.D/nn] 10.1.0.45/24

Enter the name of the GE interface that you want the scsirouter instance to use.
Scsirouter instance GE interface ? [ge1|ge2 (ge1)] ge2

Please wait ...

Now discovering all FC devices connected to the SN 5428-2-K9...

A scsirouter has been created. A list of accessible FC devices
is shown in the table below. Use the "scsirouter" command or the
configuration screen via the GUI to define one or more scsirouter targets.

Access to scsirouter targets will be disabled until access is explicitly
configured using the "scsirouter" command or the configuration
via the GUI.

Fabric Attached Devices detected
Interface WWPN                PortId  Device Type Lun  Lunid Type  Lunid
-----
fc1      2200001026448a0d 0x101e1  Disk      0  IEEE Extended 2000001026448a0d
fc1      22000003be3203bc 0x101e2  Disk      0  IEEE Extended 20000003be3203bc

Lun Description Table
Interface WWPN                Lun  Capacity Vendor  Product  Serial
-----
fc1      2200001026448a0d 0  17GB  SEAGATE  ST217340EB  2BB01L3J0000600256BW
fc1      22000003be3203bc 0  17GB  SEAGATE  ST217341EB  2DU0537A00006105FGJ6

scsirouter setup is complete.

Done with setup.
```


Related Commands	Command	Description
	clear conf	Return most configuration settings to factory defaults.
	setup	Run the setup configuration wizard.
	setup access	Run the wizard to configure Monitor mode and Administrator mode passwords.
	setup cluster	Change the configuration of the high availability environment.
	setup fcip	Run the wizard to manually configure FCIP instances.
	setup iscsi-port	Run the wizard to manually configure the port used for iSCSI traffic.
	setup mgmt	Run the wizard to configure the management interface.
	setup netmgmt	Run the wizard to configure network management.
	setup time	Run the wizard to configure the system date and time.

setup time

To set current date and time information and other time-related configuration settings, use the **setup time** configuration wizard. The storage router uses date and time information for log files and the user interface.

setup time [*parameter1 parameter2...*]

Syntax Description

<i>parameter1 parameter2 ...</i>	(Optional) Enter each parameter that the wizard prompts for. All parameters must be passed. If a parameter includes an embedded space, enclose the parameter in quotation marks.
----------------------------------	--

Defaults

Defaults or current values are shown in parentheses within the allowable response brackets. In the following example, the current date is *02/05/2002*.

Date (mm/dd/yyyy)? [02/05/2002]

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The wizard prompts you to enter the appropriate time zone (as an offset from Universal/GMT). You can also enter an optional IP address of an NTP server, to be used by the storage router for date and time synchronization. If no NTP server address is provided, the wizard prompts you for the current date and time.

Only one setup wizard can be active at any given time. Multiple users cannot run multiple setup wizards concurrently.

Use the optional *parameter* arguments to run the **setup time** wizard from a command script. All parameters required by the wizard must be included. The **setup time** wizard will not complete unless all parameters are passed.



Note

If too many parameters are passed, the **setup time** wizard will ignore the extra parameters and may complete. If a parameter is not in the correct format or is otherwise invalid, the next parameter is used to attempt to fulfill the prompt. In either case, unexpected results could occur. Always check the output from a **setup time** command when using the *parameter* arguments.

Examples

The following shows example output and input for the **setup time** command:

```
[SN5428-2A]# setup time
```

```
#####
## Date and Time Setup ##
#####
```

To provide correct information in log files and user interfaces, the SN5428-2 must have a reasonably accurate date and time.

To use Daylight Savings Time or specify time zone by geographic region use the "clock timezone" command.

The time zone must be entered as an offset from GMT.

```
0=[0000 GMT]      1=[-0100 WAT]    2=[-0200 AT]
3=[-0300 Brazil]  4=[-0400 AST]    5=[-0500 EST]
6=[-0600 CST]     7=[-0700 MST]    8=[-0800 PST]
9=[-0900 YST]     10=[-1000 AHST]  11=[-1100 NT]
12=[+1200 IDLW]   13=[+1100 WST]   14=[+1000 GST]
15=[+0900 JST]    16=[+0800 CCT]   17=[+0700 WAST]
18=[+0600 ZP6]    19=[+0500 ZP5]   20=[+0400 ZP4]
21=[+0300 BT]     22=[+0200 EET]   23=[+0100 CET]
```

```
Time Zone? [0-23] 6
```

If a Network Time Protocol (NTP) server is in use on a network reachable via the SN5428-2 management interface, it may be used to keep the SN5428-2 date and time in sync with the rest of the network.

```
NTP Server IP Address? [A.B.C.D] 10.1.60.86
```

If you enter the NTP server IP address, the date and time is synchronized with the network and the wizard completes. If you do not enter an NTP server IP address, the wizard prompts you for the current date and time information.

```
NTP Server IP Address? [A.B.C.D]
```

```
Date (mm/dd/yyyy)? [02/05/2002]
```

```
Time (hh:mm:ss)? [16:42:38] 10:42:12
```

Date and time are now configured.

Done with setup.

Related Commands	Command	Description
	<code>clear conf</code>	Return most configuration settings to factory defaults.
	<code>setup</code>	Run the setup configuration wizard.
	<code>setup access</code>	Run the wizard to configure Monitor mode and Administrator mode passwords.
	<code>setup cluster</code>	Change the configuration of the high availability environment.
	<code>setup fcip</code>	Run the wizard to manually configure FCIP instances.
	<code>setup iscsi-port</code>	Run the wizard to manually configure the port used for iSCSI traffic.
	<code>setup mgmt</code>	Run the wizard to configure the management interface.
	<code>setup netmgmt</code>	Run the wizard to configure network management.
	<code>setup scsi</code>	Run the wizard to configure a SCSI routing instance.

show aaa

To display AAA configuration information and operational statistics, use the **show aaa** command.

show aaa [**from** {*filename* | **bootconfig** | **runningconfig**}]

show aaa [**stats**]

Syntax Description	from <i>filename</i>	(Optional) The name of the configuration file where the AAA configuration is stored. This file must exist in the <i>savedconfig</i> directory.
	from bootconfig	(Optional) Display the AAA information from the persistent saved configuration.
	from runningconfig	(Optional) Display the AAA information from the currently running configuration.
	stats	(Optional) Display the number of authentication requests received and sent since the storage router was last rebooted.

Defaults	If no from parameter is specified, the display shows information from the currently running configuration.
----------	---

Command Modes	Administrator or Monitor.
---------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.
	3.3.1	The from , bootconfig , and runningconfig keywords and the <i>filename</i> argument were added.

Usage Guidelines	Use this command to display the current AAA configuration for the storage router. Use the stats keyword to display usage statistics. Use the from bootconfig keywords to display the specified AAA configuration information as it exists in the current saved configuration, used when the storage router restarts. This may differ from the running configuration.
------------------	--

Examples	The following example output displays the current AAA authentication configuration for the storage router from the persistent saved configuration. The iSCSI default authentication list indicates that authentication first tries to contact TACACS+ servers. If no server is found, TACACS+ returns an error and AAA tries to use the local username database for authentication. If a match is found, the IP host is allowed access; if no match is found, the IP host is denied access. If this attempt returns an error, the IP host is not allowed access.
----------	--


```
[SN5428-2A]# show aaa from bootconfig
aaa new-model
aaa authentication iscsi default group tacacs+ local
username "fred" password "9 af4f2428498a41a31e237de1c4a9b9fcef"
username "pat" password "9 7ddbccc3d0daf013f4293c3d3bd94539dd"
username "kris" password "9 0607167520058771e66ab1d379d7e6505f"
username "adrian" password "9 0ad24a3b35dc296d894e512416d572b3ee"
radius-server retransmit 12
radius-server host 10.5.0.53 auth-port 1645
tacacs-server timeout 12
tacacs-server host 10.7.0.22 auth-port 49
```

The following is example output from the **show aaa stats** command:

```
[SN5428-2A]# show aaa stats
authentication requests received =      134
authentication responses sent    =      134
authentication requests canceled =        0
authentication requests passed   =     130
authentication requests failed   =         4

      RADIUS Server Hosts
  IP Address    port  timeouts  bad resps
-----
    10.5.0.53   1645         0         0

      TACACS+ Server Hosts
  IP Address    port  timeouts  bad resps
-----
    10.7.0.22   49         0         0
```

Related Commands

Command	Description
aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
debug aaa	Enable debugging for the AAA authentication services.
radius-server host	Configure remote RADIUS servers for AAA authentication services.
restore aaa	Restore AAA authentication services from the named configuration file.
save aaa	Save the current AAA configuration information.
tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.
username password	Add a user name and optional password to the local username database.

show accesslist

To display a list of access lists or the contents of the named access list (or all access lists), use the **show accesslist** command.

```
show accesslist [name | all] [from {filename | bootconfig | runningconfig}]
```

Syntax Description

<i>name</i>	(Optional) The name of the access list.
all	(Optional) Display all access list entries.
from <i>filename</i>	(Optional) The name of the configuration file where the access list configuration is stored. This file must exist in the <i>savedconfig</i> directory.
from bootconfig	(Optional) Display the access list information from the persistent saved configuration.
from runningconfig	(Optional) Display the access list information from the currently running configuration.

Defaults

If no **from** parameter is specified, the display shows information from the currently running configuration.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

- Use the **show accesslist** command to display a list of all access lists from the current running configuration.
- Use the **all** keyword to display the contents of all access lists.
- Use the **from bootconfig** keywords to display the specified access list information as it exists in the current saved configuration, used when the storage router restarts. This may differ from the running configuration.

Examples

To display a list of access lists, issue this command:

```
[SN5428-2A]# show accesslist
```

To display the contents of all access lists from the current running configuration, issue this command:

```
[SN5428-2A]# show accesslist all
```

To display the contents of all access lists as they exist in the current bootable configuration, issue this command:

```
[SN5428-2A]# show accesslist all from bootconfig
```


To display the contents of the access list named *webserver2* from the current running configuration, issue this command:

```
[SN5428-2A] # show accesslist webserver2
```

To display the contents of the access list named *webserver2* as it exists in the saved configuration file *backup_1218*, issue this command:

```
[SN5428-2A] # show accesslist webserver2 from backup_1218
```

Related Commands

Commands	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
accesslist chap-username	Add CHAP user name entries to an access list.
accesslist iscsi-name	Add iSCSI Name entries to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.

show admin

To display the system administrator contact information, use the **show admin** command.

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The following information displays:

- Contact name
- E-mail address
- Phone number
- Pager number

Examples

The following example displays the system administrator contact information:

```
[SN5428-2A]# show admin
Administrator Contact Information
      Name: Pat Hurley
      Email: phurley@abc123z.com
      Phone: 123.456.7890
      Pager: 123.456.3444 pin 2234
```

Related Commands

Command	Description
admin contactinfo	Configure the storage router administrator contact information.

show boot

To display system boot information and startup file parameters, use the **show boot** command.

show boot

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator or Monitor.
----------------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to view system boot information, such as the boot device type, path to the boot image, and path to the file containing the startup commands. The show boot command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.
-------------------------	---

Examples	The following example displays system boot information:
-----------------	---

```
[SN5428-2A]# show boot
  Boot Device: ata=0,00
    Boot File: /ata0/vxWorks
  Startup File: /ata0/NuSpeed.start
    Flags: 0x0
    Other: fei
```

Related Commands	Command	Description
	show software version	Display a list of software versions available on the storage router, including the currently running version and the version that will run the next time the storage router is restarted.

show bootconfig

To display the bootable configuration for the SN 5428-2 Storage Router, or to save the commands used to create the bootable configuration to a file, use the **show bootconfig** command.

show bootconfig [*to filename*]

Syntax Description

to filename	(Optional) Save the bootable configuration as a series of CLI commands and descriptive text to the specified file. The file will be saved in the <i>script</i> directory.
--------------------	---

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use the **to** keyword to save the bootable configuration as a series of CLI commands and descriptive text in the specified file. This file is saved in the *script* directory and can be used as a basis to create command scripts to automate common tasks. Use the **read script** command to execute a command script.



Note

A saved configuration file requires editing before it can be used as a command script via the **read script** command.

[Table 12-20](#) describes the significant elements that are displayed:

Table 12-20 Elements Displayed for the “show bootconfig” Command

Element	Description
AAA	Authentication, authorization, and accounting method configuration information.
ACCESSLIST	Access list description and entry information.
ADMIN	The storage router administrator contact information.
ADMIN LOGIN	The Administrator mode password.
CDP	Cisco Discovery Protocol configuration, including timer and holdtime settings.
CLUSTER	The name of the cluster to which this storage router belongs.
DNS	The name of any defined domain name servers.
FCIP	FCIP instance configuration information.

Table 12-20 Elements Displayed for the “show bootconfig” Command (continued)

Element	Description
FC PORTS	Operational characteristics of the Fibre Channel interfaces.
FC SWITCH	Global Fibre Channel attributes.
FC ZONE	Zone configuration information.
FC ZONE ALIAS	Zone alias configuration information.
FC ZONE SET	Zone set configuration information.
GE	IP addresses and operational characteristics of the Gigabit Ethernet interfaces.
HA	HA configuration information.
HA Port	IP address and operational characteristics of the HA interface.
LOGGING ROUTE FACILTIY	The logging table.
Mgmt Port	IP address and operational characteristics of the management interface.
MONITOR LOGIN	The Monitor mode password.
RESTRICT	Storage router interface restrictions.
RIP	Routing Information Protocol (RIP) configuration information.
ROUTES	The routing table.
SCSIROUTER	Configuration information for each SCSI routing instance, including name, description, server interface and other instance-specific configuration information.
SNMP	The SNMP settings.
SNTP	Date and time information, including the address of any associated NTP server.
SOFTWARE	The default download location for storage router software.
SSH	Secure Shell (SSH) configuration information.
SYSLOG	Remote logging configuration information.
SYSTEM	SN 5428-2 Storage Router name.
TELNET	Session timeout information.
VLAN	VLAN configuration information.
VTP DOMAIN	VTP domain name.
VTP MODE	VTP configuration mode.

Examples

The following is example output from the **show bootconfig** command, for a storage router deployed for SCSI routing:

```
[SN5428-2A] # show bootconfig
!
! CLUSTER
!
! cluster Lab1
!
! ACCESSLIST
```



```

!
accesslist aegis
accesslist aegis 10.2.0.23/255.255.255.255
accesslist aegis 10.3.0.36/255.255.255.255
accesslist aegis 10.4.0.49/255.255.255.255
accesslist aegis iscsi-name ign.1987-05.com.cisco.08.80342789af73ebcdef123.xxx
accesslist aegis iscsi-name ign.1987-05.com.cisco.08.7125abc9af73ebcdef123.xxx
accesslist aegis iscsi-name ign.1987-05.com.cisco.08.1234abecf9876bac00034.xxx
accesslist aegis chap-username 12h7b.lab2.webservices
accesslist aegis chap-username dorothy
accesslist aegis chap-username lab2servp
!
! VTP DOMAIN
!
vtp domain none
!
! VTP MODE
!
vtp mode client
!
! VLAN
!
! (no vlan(s) found)
!
! SCSIROUTER
!
scsirouter zeus
scsirouter zeus authenticate "none"
scsirouter zeus primary "none"
scsirouter zeus reserve proxy disable
scsirouter zeus failover primary none
scsirouter zeus failover secondary none
scsirouter zeus lun reset no
scsirouter zeus serverIf ge1 10.1.0.45/255.255.255.0
scsirouter zeus target webserver2 wwpn "21:00:00:05:ae:03:6d:6e"
scsirouter zeus target webserver2 enabled
scsirouter zeus target webserver2 accesslist "aegis" rw
scsirouter zeus target webserver2 accesslist "any" ro
!
! SYSTEM
!
hostname SN5428-2A
!
! Mgmt Port
!
interface mgmt ip-address 10.1.10.244/255.255.255.0
!
! HA Port
!
interface ha ip-address 10.1.20.56/255.255.255.0
!
! GE
!
interface ge1 autonegotiation autodetect
interface ge1 mtusize 1500
interface ge1 vlan enable
!
! GE
!
interface ge2 autonegotiation autodetect
interface ge2 mtusize 1500
interface ge2 vlan enable
!
! ROUTES

```



```
!  
ip route 10.1.30.0/255.255.255.0 10.1.10.201  
ip route 10.1.40.243/255.255.255.255 10.1.10.201  
ip route 10.1.50.249/255.255.255.255 10.1.10.201  
ip default-gateway 10.1.10.201  
!  
! RIP  
!  
no ip rip enable  
ip rip timers invalid 180  
!  
! ADMIN  
!  
admin contactinfo name "pat"  
!  
! ADMIN LOGIN  
!  
admin password <password>  
!  
! MONITOR LOGIN  
!  
monitor password <password>  
!  
! SNMP  
!  
ntp peer 10.1.60.86  
clock timezone CST6CDT  
!  
! SNMP  
!  
snmp-server community public ro  
snmp-server community private rw  
no snmp-server host all traps  
no snmp-server sendauthtraps  
snmp-server linkupdown mgmt  
snmp-server linkupdown ge1  
snmp-server linkupdown ge2  
snmp-server linkupdown fc1  
snmp-server linkupdown fc2  
snmp-server linkupdown fc3  
snmp-server linkupdown fc4  
snmp-server linkupdown fc5  
snmp-server linkupdown fc6  
snmp-server linkupdown fc7  
snmp-server linkupdown fc8  
!  
! DNS  
!  
ip name-server 10.1.40.243 10.1.50.249  
ip domain-name mystoragenet.com  
!  
! TELNET  
!  
no session-timeout  
!  
! SSH  
!  
ssh enable  
!  
! SOFTWARE  
!  
software http url "http://www.cisco.com"  
software http username "ciscocustomer" password "<password>"  
software proxy username none
```



```

!
! HA
!
! ha configuration clustered
!
! SYSLOG
!
logging syslog 10.1.40.251
!
! LOGGING ROUTE FACILITY
!
logging level notice from all to all
logging level info from all to logfile

!
! RESTRICT
!
restrict mgmt ftp
no restrict mgmt telnet
no restrict mgmt http
no restrict mgmt snmp
restrict mgmt ssl
no restrict mgmt ssh
!
restrict ha ftp
restrict ha telnet
no restrict ha http
no restrict ha snmp
restrict ha ssl
restrict ha ssh
!
restrict ge1 ftp
restrict ge1 telnet
restrict ge1 http
restrict ge1 snmp
restrict ge1 ssl
restrict ge1 ssh
!
restrict ge2 ftp
restrict ge2 telnet
restrict ge2 http
restrict ge2 snmp
restrict ge2 ssl
restrict ge2 ssh
!
! CDP
!
cdp enable
cdp timer 60
cdp interface mgmt enable
cdp interface ha enable
cdp interface ge1 enable
cdp interface ge2 enable
!
! FC SWITCH
!
fcswitch ratov 10000
fcswitch edtov 2000
fcswitch dstov 5000
fcswitch fstov 1000
fcswitch zoning default all
fcswitch zoning autosave enable
fcswitch zoning merge SW2
fcswitch domainid 1 force

```



```
no fcswitch domainid lock enable
fcswitch interop-credit 12
!
! FC ZONE ALIAS
!
fcalias iscsi
fcalias iscsi member wwpn 280000048aa58710
fcalias iscsi member wwpn 290000048aa58710
fcalias leto
fcalias leto member wwpn 201b00491585c219
!
! FC ZONE
!
zone agamemnon
zone agamemnon member wwpn 201b00491585c219
zone agamemnon member fcalias leto
!
! FC ZONE SET
!
zoneset helen
zoneset helen zone agamemnon
no zoneset helen enable
!
! FC PORTS
!
interface fc1 enable
interface fc1 ms-enable enable
no interface fc1 al-fairness enable
interface fc1 fan-enable enable
interface fc1 ext-credit 0
interface fc1 mfs-bundle enable timeout 10
interface fc1 linkspeed auto
interface fc1 type gl-port
!
interface fc2 enable
interface fc2 ms-enable enable
no interface fc2 al-fairness enable
interface fc2 fan-enable enable
interface fc2 ext-credit 0
interface fc2 mfs-bundle enable timeout 10
interface fc2 linkspeed auto
interface fc2 type gl-port
!
interface fc3 enable
interface fc3 ms-enable enable
no interface fc3 al-fairness enable
interface fc3 fan-enable enable
interface fc3 ext-credit 0
interface fc3 mfs-bundle enable timeout 10
interface fc3 linkspeed auto
interface fc3 type gl-port
!
interface fc4 enable
interface fc4 ms-enable enable
no interface fc4 al-fairness enable
interface fc4 fan-enable enable
interface fc4 ext-credit 0
interface fc4 mfs-bundle enable timeout 10
interface fc4 linkspeed auto
interface fc4 type gl-port
!
```



```

interface fc5 enable
interface fc5 ms-enable enable
no interface fc5 al-fairness enable
interface fc5 fan-enable enable
interface fc5 ext-credit 0
interface fc5 mfs-bundle enable timeout 10
interface fc5 linkspeed auto
interface fc5 type gl-port
!
interface fc6 enable
interface fc6 ms-enable enable
no interface fc6 al-fairness enable
interface fc6 fan-enable enable
interface fc6 ext-credit 0
interface fc6 mfs-bundle enable timeout 10
interface fc6 linkspeed auto
interface fc6 type gl-port
!
interface fc7 enable
interface fc7 ms-enable enable
no interface fc7 al-fairness enable
interface fc7 fan-enable enable
interface fc7 ext-credit 0
interface fc7 mfs-bundle enable timeout 10
interface fc7 linkspeed auto
interface fc7 type gl-port
!
interface fc8 enable
interface fc8 ms-enable enable
no interface fc8 al-fairness enable
interface fc8 fan-enable enable
interface fc8 ext-credit 0
interface fc8 mfs-bundle enable timeout 10
interface fc8 linkspeed auto
interface fc8 type gl-port
!
! AAA
!
aaa new-model
username "fred" password "9 af4f2428498a41a31e237de1c4a9b9fcef"
username "pat" password "9 7ddbccc3d0daf013f4293c3d3bd94539dd"
username "kris" password "9 0607167520058771e66ab1d379d7e6505f"
username "adrian" password "9 0ad24a3b35dc296d894e512416d572b3ee"
radius-server retransmit 12
radius-server host 10.5.0.53 auth-port 1645
radius-server host 10.6.0.61 auth-port 1645
radius-server host 10.7.0.62 auth-port 1645
tacacs-server timeout 12
tacacs-server host 10.7.0.22 auth-port 49
aaa group server radius "testradius"
aaa group server radius "testradius" server 10.5.0.53 auth-port 1645
aaa group server radius "testradius" server 10.6.0.61 auth-port 1645
aaa authentication iscsi default local group radius local-case
aaa authentication iscsi test group testradius local
aaa authentication enable default group radius enable
aaa authentication login default group radius monitor

```

The following example creates a command file called *SN5428-2AScript1* in the *script* directory. It contains many of the CLI commands that were issued to create the current bootable configuration.

```
[SN5428-2A]# show bootconfig to SN5428-2AScript1
```


Related Commands	Command	Description
	read script	Read and execute the CLI commands in the named script file.
	restore all	Restore the contents of the named configuration file into memory.
	save all	Save all configuration information
	show runningconfig	Display the running configuration, or create a command file based on the running configuration.
	show savedconfig	List the contents of the savedconfig directory or the contents of the named configuration file.
	show script	Display the contents of the script directory or the contents of the named command file.

show buffers

To display buffer pool information for a variety of areas, use the **show buffers** command.

show buffers

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator or Monitor.
----------------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	The display includes the number of free memory buffers for each pool, along with those currently allocated to various functions. The show buffers command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.
-------------------------	---

Examples	The following is sample output from the show buffers command:
-----------------	--

```
[SN520A]# show buffers
Pool System:
```

```

type          number
-----
FREE      :    42086
DATA      :         0
HEADER    :         0
SOCKET    :        14
PCB       :        21
RTABLE    :        31
HTABLE    :         0
ATABLE    :         0
SONAME    :         0
ZOMBIE    :         0
SOOPTS    :         0
FTABLE    :         0
RIGHTS    :         0
IFADDR    :        18
CONTROL   :         0
OObDATA   :         0
IPMOPTS   :         1
IPMADDR   :         5
IFMADDR   :         0
MRTABLE   :         0
TOTAL     :    42176
LOW WTR   :    42082
```



```

number of mbufs: 42176
number of times failed to find headers: 0
number of times failed to find clusters: 0
number of times waited for space: 0
number of times drained protocols for space: 0

```

CLUSTER POOL TABLE

size	clusters	free	usage	low water
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----

Pool iSCSI:

type	number
-----	-----

```

FREE      :    3240
DATA      :         0
HEADER    :         0
SOCKET    :         0
PCB       :         0
RTABLE    :         0
HTABLE    :         0
ATABLE    :         0
SONAME    :         0
ZOMBIE    :         0
SOOPTS    :         0
FTABLE    :         0
RIGHTS    :         0
IFADDR    :         0
CONTROL   :         0
OOBDATA   :         0
IPMOPTS   :         0
IPMADDR   :         0
IFMADDR   :         0
MRTABLE   :         0
TOTAL     :    3240
LOW WTR   :    3240

```

```

number of mbufs: 3240
number of times failed to find headers: 0
number of times failed to find clusters: 0
number of times waited for space: 0
number of times drained protocols for space: 0

```

CLUSTER POOL TABLE

size	clusters	free	usage	low water
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----

Output from CPP

Pool System:

type	number
-----	-----

```

FREE      :    6240
DATA      :         0
HEADER    :         0
SOCKET    :        31
PCB       :        48
RTABLE    :        36
HTABLE    :         0
ATABLE    :         0

```


■ show buffers

```

SONAME      :      0
ZOMBIE      :      0
SOOPTS      :      0
FTABLE      :      0
RIGHTS      :      0
IFADDR      :     12
CONTROL     :      0
OOBDATA     :      0
IPMOPTS     :      5
IPMADDR     :     12
IFMADDR     :      0
MRTABLE     :      0
TOTAL       :    16384
LOW WTR     :    16224
number of mbufs: 16384
number of times failed to find headers: 0
number of times failed to find clusters: 0
number of times waited for space: 0
number of times drained protocols for space: 0

```

CLUSTER POOL TABLE

size	clusters	free	usage	low water
64	1449	1412	50	1408
128	1688	1643	76660	1637
256	1847	1822	36	1817
512	1941	1910	76646	1904

Pool Data:

```

type        number
-----
FREE       :    16800
DATA       :      0
HEADER     :      0
SOCKET     :      0
PCB        :      0
RTABLE     :      0
HTABLE     :      0
ATABLE     :      0
SONAME     :      0
ZOMBIE     :      0
SOOPTS     :      0
FTABLE     :      0
RIGHTS     :      0
IFADDR     :      0
CONTROL    :      0
OOBDATA    :      0
IPMOPTS    :      0
IPMADDR    :      0
IFMADDR    :      0
MRTABLE    :      0
TOTAL      :    16800
LOW WTR    :    16386
number of mbufs: 16800
number of times failed to find headers: 0
number of times failed to find clusters: 0
number of times waited for space: 0
number of times drained protocols for space: 0

```


CLUSTER POOL TABLE

size	clusters	free	usage	low water
64	2832	2832	58994	2816
128	4124	4124	367277	3946
256	901	901	138752	770
512	947	947	67656	857
1024	96	96	37952	68
2048	97	97	1051	96

Net Buffers:

type	number
FREE	: 12798
USED	: 2
TOTAL	: 12800

Related Commands

Command	Description
show stack	Display the memory stack on a per-task basis.
show tech-support	Display a variety of diagnostic information for use by Cisco Technical Support professionals.

show cdp

To display global Cisco Discovery Protocol (CDP) configuration information for the SN 5428-2 Storage Router, including timer and holdtime information, use the **show cdp** command.

show cdp

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines This command displays current CDP configuration. Use this command to determine if CDP is enabled, and view packet timing and holdtime information. CDP allows network applications to learn device-type information and the SNMP agent address of neighboring devices.

Examples The following example displays CDP configuration information for the storage router. It shows that CDP is enabled and packets are sent every minute. The storage router directs its neighbors to hold its CDP advertisements for 3 minutes (the default CDP **holdtime** value). The storage router is also enabled to send CDP version 2 advertisements.

```
[SN5428-2A]# show cdp
Global CDP information:
  CDP is enabled
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements are enabled
```

Table 12-21 describes the significant fields shown in the display.

Table 12-21 Description of Fields in the “show cdp” Command Output

Field	Definition
Sending CDP packets every <i>nn</i> seconds	The interval (in seconds) between transmissions of CDP advertisements. This field is controlled by the cdp timer command.

Table 12-21 Description of Fields in the “show cdp” Command Output (continued)

Field	Definition
Sending a holdtime value of <i>nn</i> seconds	The amount of time (in seconds) the storage router directs a neighbor to hold the CDP advertisement before discarding it. This field is controlled by the cdp holdtime command.
Sending CDPv2 advertisements are enabled	Indicates that CDP version 2 advertisements are enabled.

Related Commands

Command	Description
cdp enable	Enable or disable CDP on the SN 5428-2 Storage Router.
cdp holdtime	Specify the amount of time the receiving device should hold a CDP packet from the SN 5428-2 Storage Router before discarding it.
cdp interface	Switch CDP on or off for the specified interface.
cdp timer	Specify the amount of time between transmissions of CDP packets from the SN 5428-2 Storage Router.
show cdp entry	Display information about a specific neighbor device listed in the CDP neighbors table.
show cdp interface	Display information about the storage router interfaces on which CDP is enabled.
show cdp neighbors	Display detailed information about neighboring devices discovered using CDP.
show cdp traffic	Display information about traffic between devices gathered using CDP.

show cdp entry

To display information about a specific neighboring device or all neighboring devices discovered using CDP, use the **show cdp entry** command.

```
show cdp entry {device-id | all}
```

Syntax Description	<i>device-id</i>	The device ID of the CDP neighbor about which you want information.
	all	Display all CDP neighbors.

Defaults	None.
----------	-------

Command Modes	Administrator or Monitor.
---------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to display operational information about CDP neighbors known to the storage router. Use show cdp neighbors command to display the device ID for the neighbor about which you want additional information.
------------------	---

Examples	The following is sample output from the show cdp entry command. Information about all neighboring devices is displayed, including device ID, address and protocol, platform, interface, holdtime, and version.
----------	---

```
[SN5428-2A]# show cdp entry all
-----
Device ID: SCA0428017Q(lab-SN5428-2A.mylab.com)
Entry address(es):
  IP address: 10.2.1.28
Platform: WS-C6509, Capabilities: Trans-Bridge Switch IGMP
Interface: ge2, Remote Port (outgoing port): 4/13
Holdtime : 176 sec

Version :
WS-C6509 Software, Version McpSW: 6.1(1b) NmpSW: 6.1(1b)
Copyright (c) 1995-2000 by Cisco Systems

advertisement version: 1
```


Related Commands	Command	Description
	cdp enable	Enable or disable CDP on the SN 5428-2 Storage Router.
	cdp holdtime	Specify the amount of time the receiving device should hold a CDP packet from the SN 5428-2 Storage Router before discarding it.
	cdp interface	Switch CDP on or off for the specified interface.
	cdp timer	Specify the amount of time between transmissions of CDP packets from the SN 5428-2 Storage Router.
	show cdp	Display global CDP configuration information for the storage router.
	show cdp interface	Display information about the storage router interfaces on which CDP is enabled.
	show cdp neighbors	Display detailed information about neighboring devices discovered using CDP.
	show cdp traffic	Display information about traffic between devices gathered using CDP.

show cdp interface

To display information about the SN 5428-2 Storage Router interfaces on which CDP is enabled, use the **show cdp interface** command.

show cdp interface [*if-name*]

Syntax Description	<i>if-name</i>	Display CDP status and operational information for the specified interface. The following are valid interface names: mgmt, ha, ge1 and ge2.
--------------------	----------------	---

Defaults	None.
----------	-------

Command Modes	Administrator or Monitor.
---------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	CDP can be enabled for all storage router interfaces, including the management, high availability, and Gigabit Ethernet interfaces. Use the show cdp interface command to display a brief summary of all interfaces on which CDP is enabled. To display status and operational information for a specific interface, add the interface name argument.
------------------	--

Examples	The following is example output from the show cdp interface command:
----------	---

```
[SN5428-2A]# show cdp interface
Port      CDB Status
-----
mgmt      enabled
ha         enabled
ge1       enabled
ge2       enabled
```

The following is example output for the management interface (*mgmt*):

```
[SN5428-2A]# show cdp interface mgmt
Port      CDB Status
-----
mgmt      enabled
```


Related Commands	Command	Description
	cdp enable	Enable or disable CDP on the SN 5428-2 Storage Router.
	cdp holdtime	Specify the amount of time the receiving device should hold a CDP packet from the SN 5428-2 Storage Router before discarding it.
	cdp interface	Switch CDP on or off for the specified interface.
	cdp timer	Specify the amount of time between transmissions of CDP packets from the SN 5428-2 Storage Router.
	show cdp	Display global CDP configuration information for the storage router.
	show cdp entry	Display information about a specific neighbor device listed in the CDP neighbors table.
	show cdp neighbors	Display detailed information about neighboring devices discovered using CDP.
	show cdp traffic	Display information about traffic between devices gathered using CDP.

show cdp neighbors

To display detailed information about neighboring devices discovered using CDP, use the **show cdp neighbors** command.

show cdp neighbors [**interface** *if-name*] [**detail**]

Syntax Description

interface <i>if-name</i>	(Optional) Keyword and name of the interface connected to the neighbors for which you want information.
detail	(Optional) Display detailed information about a neighbor (or neighbors) including network address, enabled protocols, holdtime, and software version.

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use the **show cdp neighbors** command to display brief or detailed information about neighboring devices discovered using CDP. Add the **interface** keyword and the interface name to limit the display to neighbors connected to that specific interface.

Use the **detail** keyword to display detailed information about all devices, or devices connected to the specified interface.

Examples

The following is example output from the **show cdp neighbors** command:

```
[SN5428-2A]# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device-ID          Capability Platform      Remote Port
-----
SCA05600126(kal6-lab-swa.cm TSI      WS-C6509      4/16
SCA05600126(kal6-lab-swa.cm TSI      WS-C6509      4/12
JAB04140GZC(kal6-lab-z4-swa TS       WS-C2948      1/23
```


Table 12-22 describes the significant fields shown in the display.

Table 12-22 Description of Fields in the “show cdp neighbors” Command Output

Field	Description
Capability Codes	The type of device that can be discovered.
Device-ID	The name of the neighbor device and either the MAC address or the serial number of this device. This field is truncated after 27 characters.
Capability	The type of the device listed in the CDP Neighbors table. Possible values are: <ul style="list-style-type: none"> • R—Router • T—Transparent bridge • B—Source-routing bridge • S—Switch • H—Host • I—IGMP device • r—Repeater
Platform	The product number of the device. This field is truncated after 21 characters.
Remote Port	The outgoing port information.

The following is sample output for one neighbor from the **show cdp neighbors detail** command. The output includes additional information about the neighbor, including network address, enabled protocols, and software version.

```
[SN5428-2A]# show cdp neighbors detail
-----
Device ID: TRC0448016Q(lab-sn5428-2a.mlab.com)
Entry address(es):
  IP address: 10.2.0.83
Platform: WS-C6509, Capabilities: Trans-Bridge Switch IGMP
Interface: mgmt, Remote Port (outgoing port): 7/48
Holdtime : 138 sec

Version :
WS-C6509 Software, Version McpSW: 6.1(1b) NmpSW: 6.1(1b)
Copyright (c) 1995-2000 by Cisco Systems

advertisement version: 2
VTP Management Domain: 'LAB-SN5428-2A'
Native VLAN: 220
Duplex: half
-----
Device ID: 000421b45a00(lab32)
Entry address(es):
  IP address: 10.2.0.185
Platform: SN5428-2, Capabilities: Router
Interface: mgmt, Remote Port (outgoing port): fei0
Holdtime : 174 sec

Version :
Cisco SN5428-2 Software Version 3.2.1

advertisement version: 2
```


Table 12-23 describes the significant fields shown in the display.

Table 12-23 Description of Fields in the “show cdp neighbors detail” Command Output

Field	Description
Device-ID	The name of the neighbor device and either the MAC address or the serial number of this device.
Entry address(es)	A list of network addresses of neighbor devices.
IP address	The IP address of the neighboring device.
Platform	The product number of the device.
Capabilities	The device type of the neighbor. This device can be a router, a bridge, a transparent bridge, a source-routing bridge, a switch, a host, an IGMP device, or a repeater.
Interface	The storage router interface used to connect to this neighbor.
Remote Port	The outgoing port number.
Holdtime	The remaining amount of time (in seconds) the current device will hold the CDP advertisement from a sending device before discarding it.
Version	The software version of the neighbor device.
advertisement version	The CDP advertisement version.
VTP Management Domain	The name of the VTP management domain.
Native VLAN	The native VLAN identification number.
Duplex	The duplex state of the connection between the storage router and the neighbor device.

Related Commands

Command	Description
cdp enable	Enable or disable CDP on the SN 5428-2 Storage Router.
cdp holdtime	Specify the amount of time the receiving device should hold a CDP packet from the SN 5428-2 Storage Router before discarding it.
cdp interface	Switch CDP on or off for the specified interface.
cdp timer	Specify the amount of time between transmissions of CDP packets from the SN 5428-2 Storage Router.
show cdp	Display global CDP configuration information for the storage router.
show cdp entry	Display information about a specific neighbor device listed in the CDP neighbors table.
show cdp interface	Display information about the interfaces on which CDP is enabled.
show cdp traffic	Display information about traffic between devices gathered using CDP.

show cdp traffic

To display information about traffic between devices gathered using Cisco Discovery Protocol (CDP), use the **show cdp traffic** command.

show cdp traffic

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator or Monitor.
----------------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to view statistics about CDP traffic between the storage router and other devices.
-------------------------	---

Examples	The following is example output from the show cdp traffic command.
-----------------	--

```
[SN5428-2A]# show cdp traffic
CDP counters :
  Total packets output: 4968, Input: 22329
  Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
  No memory: 0, Invalid packet: 0, Fragmented: 0
  CDP version 1 advertisements output: 1242, Input: 9911
  CDP version 2 advertisements output: 3726, Input: 12418
```

Table 12-24 describes the fields shown in the display.

Table 12-24 Description of Fields in the “show cdp traffic” Command Output

Field	Description
Total packets output	The number of CDP advertisements sent by the storage router. This value is the sum of the “CDP version 1 advertisements output” and “CDP version 2 advertisements output” fields.
Input	The number of CDP advertisements received by the storage router. This value is the sum of the “CDP version 1 advertisements input” and “CDP version 2 advertisements input” fields.
Hdr syntax	The number of CDP advertisements with bad headers received by the storage router.
Chksum error	The number of times the verification operation failed on incoming CDP advertisements.

Table 12-24 Description of Fields in the “show cdp traffic” Command Output (continued)

Field	Description
Encaps failed	The number of times CDP failed to send advertisements on an interface because of a failure caused by the bridge port of the storage router.
No memory	The number of times the storage router did not have sufficient memory to store the CDP advertisements in the advertisement cache table when the storage router attempted to assemble advertisement packets for transmission or to parse them when receiving them.
Invalid packet	The number of invalid CDP advertisements received and sent by the storage router.
Fragmented	The number of times fragments or portions of a single CDP advertisement were received by the storage router instead of the complete advertisement.
CDP version 1 advertisements output	The number of CDP version 1 advertisements sent by the storage router.
Input	The number of CDP version 1 advertisements received by the storage router.
CDP version 2 advertisements output	The number of CDP version 2 advertisements sent by the storage router.
Input	The number of CDP version 2 advertisements received by the storage router.

Related Commands

Command	Description
cdp enable	Enable or disable CDP on the SN 5428-2 Storage Router.
cdp holdtime	Specify the amount of time the receiving device should hold a CDP packet from the SN 5428-2 Storage Router before discarding it.
cdp interface	Switch CDP on or off for the specified interface.
cdp timer	Specify the amount of time between transmissions of CDP packets from the SN 5428-2 Storage Router.
show cdp	Display global CDP configuration information for the storage router.
show cdp entry	Display information about a specific neighbor device listed in the CDP neighbors table.
show cdp interface	Display information about the interfaces on which CDP is enabled.
show cdp neighbors	Display detailed information about neighboring devices discovered using CDP.

show cli

To display information about the command line interface (CLI), use the **show cli** command.

show cli [*command-keyword*] [*command-keyword ... command keyword ...*]

show cli status

Syntax Description	<i>command-keyword</i>	(Optional) The first keyword in the command displays the CLI command tree for all varieties of that command.
	status	(Optional) Keyword used to display the status of the last CLI command.

Defaults	None.
-----------------	-------

Command Modes	Administrator or Monitor.
----------------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use the show cli command to display the complete CLI command tree, along with helpful information about command parameters and arguments. Use the <i>command-keyword</i> arguments to display information about a specific set of commands, such as <i>scsirouter</i> or <i>cdp</i> commands. Only valid commands and keywords will be displayed.
	The set of CLI commands and keywords that will be available to you depend on the level of authority associated with your CLI management session and the deployment option selected for the storage router during initial configuration.
	Use the status keyword to display the status of the last CLI command that was issued. A status of “0” indicates that the command completed without errors. A status of “-13” indicates that the command syntax was invalid.

Examples	The following is example output from the show cli command, showing the CLI command tree information for the ping command.
-----------------	---

```
[SN5428-2A]# show cli ping
ping
  <A.B.C.D | servername>
    numpkts
      <npkts>
        size
          <sn>
size
  <sn>
```

Send ICMP pings to a host
 IP address or hostname to ping
 Number of packets to attempt
 Integer greater than zero (Default is 5)
 Size of packet
 Integer (64..4096), default is 64
 Size of packet
 Integer (64..4096), default is 64

show cli

Related Commands

Command	Description
help	Display information about how to use the CLI.

show clock

To display the current system date and time, use the **show clock** command.

show clock

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator or Monitor.
----------------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to display the storage router date and time setting.
-------------------------	---

Examples	The following is example output from the show clock command:
-----------------	---

```
[SN5428-2A]# show clock
Thurs Mar 21 15:54:25 GMT+6 2002
```

Related Commands	Command	Description
	clock set	Set the system clock to the given date and time.
	clock timezone	Specify the storage router time zone information.
	ntp peer	Specify the name or IP address of the NTP server with which the storage router will synchronize date and time.
	setup time	Run the wizard to configure date and time information (including NTP server and time zone) associated with the storage router.

show cluster

To display operational information related to the high availability (HA) cluster, use the **show cluster** command.

show cluster

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Administrator or Monitor.

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines Use this command to display cluster information for the storage router whether it is in standalone or clustered mode.

Examples The following example displays cluster information. In this example, the storage router named SN 5428-2A belongs to a cluster.

```
[SN5428-2A]# show cluster
Cluster Name: Weblab
Cluster Changes: 2
Last Change: Tue Mar 19 04:12:51 GMT+6 2002
IP Multicast Address: 224.0.0.101
Operating Message Version: V3
Detected Configuration Errors: None

Local Node: SN5428-2A
HA Configuration: CLUSTERED
HA: up          MGMT Port: up      HA Port: up
Sent 19240 heartbeats
Rcvd 19238 heartbeats

Cluster Node List:
System Name      MGMT IP      HA IP      Last Heard From
SN5428-2A        10.1.10.244  10.1.20.56  Self
SN5428-2B        10.1.10.223  10.1.20.98  Tue Mar 18 05:17:43

Application List:
Application Name  Master on    State      Last Config Update
scsirouter/scsi1  SN5428-2A   Master     Mar 18 21:23:45
scsirouter/scsi2  SN5428-2B   Slave      Mar 18 23:21:10

AAA, Access List, & VLAN Management is on SN5428-2B
```


The following example displays cluster information about a standalone storage router:

```
[SN5428-2A]# show cluster
Cluster Name: 630041D
  Cluster Changes: 0
  Last Change: Mon Nov 19 14:09:18 GMT+6 2001
  IP Multicast Address: 224.0.0.101
  Operating Message Version: V3
  Detected Configuration Errors: None

Local Node: SN5428-2A
  HA Configuration: STANDALONE
  HA: down      MGMT Port: up      HA Port: down
  Sent 0 heartbeats
  Rcvd 0 heartbeats

Cluster Node List:
System Name      MGMT IP      HA IP      Last Heard From
SN5428-2A        10.1.10.244  no IP address  Self

Application List:
Application Name      Master on      State      Last Config Update
scsirouter/foo        SN5428-2A    Master      Jan 19 13:05:33

AAA, Access List, password & VLAN Management is on SN5428-2A
```

Table 12-25 describes the fields shown in the display.

Table 12-25 Description of Fields in the “show cluster” Command Output

Field Name	Description
Cluster Name	The name of the HA cluster.
Cluster Changes	The number of cluster changes made to this storage router since it was initially configured, or since the last clear conf command was issued.
Last Change	The date and time of the last cluster configuration change.
IP Multicast Address	The IP address used for multicast communications. IANA has assigned the multicast IP address 224.0.0.101 to the Cisco SN 5428-2 Storage Router.
Operating Message Version	The version identifier for system messages, including HA messages exchanged between storage routers in a cluster.
Detected Configuration Errors	The total number of configuration errors, if any, detected by the system.
Local Node	The name of the storage router.
HA Configuration	Indicates the configuration of HA in the storage router. Valid configurations are STANDALONE or CLUSTERED.
HA	Indicates the state of the HA application in the storage router. Valid states are <i>up</i> or <i>down</i> . If the HA configuration is STANDALONE, the HA state should be <i>down</i> .
MGMT Port	Indicates the state of the physical management port. Valid states are <i>up</i> or <i>down</i> .
HA Port	Indicates the state of the physical HA port. Valid states are <i>up</i> or <i>down</i> .
Sent . . . heartbeats	Number of heartbeats transmitted on the HA network.
Recvd . . . heartbeats	Number of heartbeats received on the HA network.

Table 12-25 Description of Fields in the “show cluster” Command Output (continued)

Field Name	Description
Cluster Node List	A list of storage routers in the cluster.
System Name	The name of the storage router.
MGMT IP	The IP address of the cluster node management interface.
HA IP	The IP address of the cluster node HA interface.
Last Heard From	The date and time the cluster node was last heard from.
Application List	A list of applications running on the storage router.
Application Name	A list of all SCSI routing instances in the cluster.
Master on	The name of the storage router currently running this SCSI routing instance.
State	The state of the SCSI routing instance on this storage router.
Last Config Update	The date and time of the last configuration change to this SCSI routing instance.
AAA, Access List, password & VLAN management is on	The name of the storage router in the cluster that currently handles access list, VLAN, AAA, and password management functions.

Related Commands

Command	Description
save all	Save all configuration information.
save system	Save selected system configuration information.
setup cluster	Change the configuration of the high availability environment.
show ha	Display HA operational statistics for the storage router or for a specific application.
show system	Display selected system information, including system name.

show cpu

To display CPU utilization information, use the **show cpu** command.

show cpu

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator or Monitor.
----------------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to view the percentage of CPU utilization for the last five seconds, the last minute, and the last five minutes. The show cpu command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.
-------------------------	--

Examples	<p>The following is example output from the show cpu command:</p> <pre>[SN5428-2A]# show cpu CPU Utilization for last 5 seconds: 1%; last 1 minute: 2%; last 5 minutes: 2%</pre>
-----------------	--

Related Commands	Command	Description
	show buffers	Display information about buffer pools.
	show memory	Display information about memory and related resources.
	show stack	Display the memory stack on a per-task basis.
	show tech-support	Display a variety of diagnostic information for use by Cisco Technical Support professionals.

show crash

To display saved crash trace information or current crash trace information, use the **show crash** command.

show crash [current]

Syntax Description	current	(Optional) Returns the current crash trace information for the running system.
Defaults	None.	
Command Modes	Administrator or Monitor.	
Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

The default crash trace file is crash-cpp.txt in the *log* directory. This file is created if the SN 5428-2 unexpectedly restarts. Use the **current** keyword to display the crash trace information as it exists for the currently running system. To save the command output, redirect the output of your console using the logging facilities for your specific console interface. Depending on your console interface and scroll buffer size, you may also be able to copy and paste the contents from your console into an ASCII text file.

The **show crash** command is designed for debug purposes and should only be used under the guidance of a Cisco Technical Support professional.

Examples

The following example displays the beginning of current crash trace information:

```
[SN5428-2A]# show crash current
#
# Crash Information (/ata4/log/tmpcrash.txt)
#

Cisco Systems Crash Trace
#
# System Information
#
Time Stamp:      Thu Mar 13 16:04:35 CST 2002
System Model:    SN5428-2
Software Version: 3.3.1-K9
#
# Exception Information
#
intContext: -1
Task:           0xffffffff
Param 1:         0xffffffff
Param 2:         0xffffffff
```



```

Panic Msg:  NULL
#
# Boot Information
#
VxWorks (for Galileo GT64260/MPC7410) version 5.4.1.
Kernel: WIND version 2.5.
Made on Dec 12 2002, 15:13:30.
Boot line:
ata=0,00(0,0):/ata0/vxWorks e=10.1.10.244:ffffff00 tn=lab2 s=/ata0/NuSpeed.start o=fei
#
#Task List#
#

```

In the following example, no saved crash trace information exists. This condition occurs when the command is issued and the storage router has never unexpectedly restarted.

```

show crash
#
# Crash Information (/ata4/log/crash-cpp.txt)
#

No crash information available

```

Related Commands

Command	Description
show buffers	Display information about buffer pools.
show memory	Display information about memory and related resources.
show stack	Display the memory stack on a per-task basis.
show tech-support	Display a variety of diagnostic information for use by Cisco Technical Support professionals.

show debug

To display a variety of debug information or perform specific troubleshooting activities, use the **show debug** command.

```
show debug {mailboxtrace | rawlundatabase} {fci? | all}
```

```
show debug portarray fci?
```

Syntax Description

<i>fci?</i>	The name of the internal Fibre Channel (FC) interface. Valid values are fci1 and fci2. When you type fci? , the CLI lists the interfaces available. You cannot specify a nonexistent interface.
all	Keyword used to display the specified debug information for all internal FC interfaces.
mailboxtrace	Display mailbox trace data.
portarray	Display all active virtual ports. This command is only available in systems deployed for transparent SCSI routing.
rawlundatabase	Display raw inquiry data from all discovered LUNs.

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to display debugging information for internal FC interfaces. The **show debug** command is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.

Examples

The following example displays raw lun database information for all targets discovered on the internal FC interface *fc11*:

```
[SN5428-2_PR]# show debug rawlunatabase fci1

Entry Address = 0xd047ab4
fabricLoginFailureCode=0x0,fabricLoginExtendedCode=0x0,fabricLoginTimeoutCode=0x0
ReportLunsLLDStatus=0x0,ReportLunsLLDStatusModifier=0x0,ReportLunsSCSIStatus=0x0,ReportLun
sASCASCQ=0x0,ReportLunsLunCount=1
InquiryLLDStatus=0x0,InquiryLLDStatusModifier=0x0,InquiryLastLunWithLLDLError=0x0,
InquirySCSIStatus=0x0,InquiryASCASCQ=0x0,InquiryLastLunWithSCSIStatusError=0x0
boolLunsNotSupported=0x0,InquiryLastLunNotSupported=0x0
loopId=0x0,masterState=0x6,slaveState=0x7,loggedIn=1,roles=1,valid=1,portId=0x104e1,scanLu
ns=0x0
numberLuns=0x1,reportAsyncEvent=0x0,node_wwn=0x20000004 0xae4122a6, port_wwn=0x21000004
0xae4322a6

lun=0, wwnn=0x20000020 0x37559b0e, reportAsyncEvent=0x0
stdInquiry data for lun=0x0
bytes0-7=0x00000332 0x8b00700a
vendorId=SEAGATE , product=ST318451FC , revision=0001 device Type=0x0
DeviceIdPage:bytes0-3= 0x0083000c,bytes4-7= 0x01030008,bytes8-11= 0x20000020
:bytes12-15= 0x37559b0e,bytes16-19=0x00800014,bytes20-23=0x33434330
S/N Page:bytes0-3= 0x00800014 s/n=3CC01M4K0000710367CX

Entry Address = 0xab1603c
fabricLoginFailureCode=0x0,fabricLoginExtendedCode=0x0,fabricLoginTimeoutCode=0x0
ReportLunsLLDStatus=0x0,ReportLunsLLDStatusModifier=0x0,ReportLunsSCSIStatus=0x0,ReportLun
sASCASCQ=0x0,ReportLunsLunCount=1
InquiryLLDStatus=0x0,InquiryLLDStatusModifier=0x0,InquiryLastLunWithLLDLError=0x0,
InquirySCSIStatus=0x0,InquiryASCASCQ=0x0,InquiryLastLunWithSCSIStatusError=0x0
boolLunsNotSupported=0x0,InquiryLastLunNotSupported=0x0
loopId=0x1,masterState=0x6,slaveState=0x7,loggedIn=1,roles=1,valid=1,portId=0x101e2,scanLu
ns=0x0
numberLuns=0x1,reportAsyncEvent=0x0,node_wwn=0x20000004 0xae4304cd, port_wwn=0x22000004
0xae4304cd

lun=0, wwnn=0x20000004 0xae4304cd, reportAsyncEvent=0x0
stdInquiry data for lun=0x0
bytes0-7=0x00000312 0x8b00700a
vendorId=SEAGATE , product=ST318452FC , revision=0002 device Type=0x0
DeviceIdPage:bytes0-3= 0x0083000c,bytes4-7= 0x01030008,bytes8-11= 0x20000004
:bytes12-15= 0xae4304cd,bytes16-19=0x00700014,bytes20-23=0x43465630
S/N Page:bytes0-3= 0x00800014 s/n=3FZ0647A00a06216DVJ7

Entry Address = 0xcb1974c
fabricLoginFailureCode=0x0,fabricLoginExtendedCode=0x0,fabricLoginTimeoutCode=0x0
ReportLunsLLDStatus=0xbfc0,ReportLunsLLDStatusModifier=0x3801,ReportLunsSCSIStatus=0x7fcb,
ReportLunsASCASCQ=0x8c13,ReportLunsLunCou7
InquiryLLDStatus=0x5179,InquiryLLDStatusModifier=0x8492,InquiryLastLunWithLLDLError=0x7a90,
InquirySCSIStatus=0xace3,InquiryASCASCQ=0x800b,InquiryLastLunWithSCSIStatusError=0xffe3
boolLunsNotSupported=0x38da7321,InquiryLastLunNotSupported=0xfc51
loopId=0x7e,masterState=0x6,slaveState=0x7,loggedIn=1,roles=0,valid=1,portId=0xfffffe,scan
Luns=0x1
numberLuns=0x0,reportAsyncEvent=0x0,node_wwn=0x10000002 0x3d071161, port_wwn=0x20000002
0x3a171241
```


Related Commands	Command	Description
	debug scsirouter	Enable debugging for the named SCSI routing instance
	debug scsirouter target	Enable debugging for a specific SCSI routing instance target and LUN combination.

show debug fcip

To display a variety of debug information or perform specific troubleshooting activities for FCIP instances, use the **show debug fcip** command.

show debug fcip *name* {**mailboxtrace** | **packettrace**}

Syntax Description

<i>name</i>	The name of the FCIP instance. Valid names are <i>fcip1</i> and <i>fcip2</i> .
mailboxtrace	Display mailbox trace data.
packettrace	Display packet trace data.
Note	The packet trace mask can be set for the current session using the debug fcip command. To retain the packet trace mask setting over a storage router restart, use the fcip destination config command.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced.

Usage Guidelines

Use this command to display debugging information for FCIP instances. The **show debug** command is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.

Examples

The following is example mailbox trace data for the FCIP instance named *fcip1*:

```
[SN5428-2A]# show debug fcip fcip1 mailboxtrace
qlpt 0xca99f98, unit 1
linkState Down, linkIsUp FALSE
Peer 0.0.0.0, isConnected TRUE
InitBlock values:
  Max IOCB Allocation 256, Max Frame Length 2112
  Execution Throttle 16, Retry Count 8
  Retry Delay 1, Inquiry Data 0
  Risc Option 0x8000, Additional Firmware Option 0x10
  Special Firmware Option 0x6000
FW_Rev 3.100.101, FW_State 0x4
pktTraceMask 0x0
mboxTracing Yes, cmdCount 0
requestQ: queue_base = 0xca92000
reqinptr = 28, reqoutptr = 0
reqInAbsAddress = 0xca92700, reqOutAbsAddress = 0xca92000
responseQ: queue_base = 0xca8c000
respinptr = 28, respoutptr = 28
respInAbsAddress = 0xca8c700, respOutAbsAddress = 0xca8c700
```


show debug fcip

```

046: 40 8 - 0
      0009 9d40 0ca8 b000 0040 0000 0000 0000 0000
047: 41 1 - 0
      4000 1111 2222 3333 4444 5555 6666 7777 ffff
048: 40 8 - 0
      0009 9d80 0ca8 b000 0040 0000 0000 0000 0000
049: 41 1 - 0
      4000 1111 2222 3333 4444 5555 6666 7777 ffff
050: 40 8 - 0
      0009 9dc0 0ca8 b000 0040 0000 0000 0000 0000
051: 41 1 - 0
      4000 1111 2222 3333 4444 5555 6666 7777 ffff
052: 40 2 - 0
      0007 0800 0ca8 b000 0040 0000 0000 0000 0000
...

```

Related Commands

Command	Description
debug fcip	Enable debugging for the named FCIP instance.
fcip	Create an FCIP instance.
fcip destination config	Configure operational parameters for the named FCIP instance.
show fcip	Display configuration and operational information for the named FCIP instance.

show debug fcswitch

To display internal Fibre Channel (FC) interface parameters, use the **show debug fcswitch** command.

show debug fcswitch {all | brief | memory | tech-support}

show debug fcswitch clish *text*

Syntax Description	all	Display all interface parameters for internal FC interfaces fc0, fc15, fci1 and fci2, including all switch log entries.
	brief	Display all interface parameters for internal FC interfaces fc0, fc15, fci1 and fci2. Includes only the last 5 switch log entries.
	memory	Display memory usage for the integrated FC switch component.
	tech-support	Display technical support information for the integrated FC switch component.
	clish <i>text</i>	Display internal operational information for the integrated FC switch component. The <i>text</i> argument is any valid switch “show” command. If the <i>text</i> argument includes spaces, enclose it in quotation marks.

Defaults	None.
----------	-------

Command Modes	Administrator or Monitor.
---------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	The show debug fcswitch command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.
	Use the show debug fcswitch brief or show debug fcswitch all commands to display initiator WWPN information (fci1 is initiator WWPN1 and fci2 is initiator WWPN2) and other parameters related to the internal FC interfaces.

Examples	The following example displays various configuration parameters for the internal FC interfaces, and the last five switch log entries:
	<pre>[SN5428-2_PR]# show debug fcswitch brief Interface WWPN switch port ----- fc0 200000021e071161 fc15 200f00021e071161</pre>

show debug fcswitch

```

Initiator Value
-----
WWPN1      280000021e071160
WWPN2      290000021e071160

Global attributes      Value
-----
Switch Name           SN5428-2
Node WWN              100000021e071151
DomainID              1
Uptime (seconds)      76956
SysLogLevel           Critical
SysLogComp            NameServer MgmtServer Zoning Switch Chassis Blade Port Eport Other
DevLogLevel           Critical
DevLogComp            None
AlarmEntries          1

Display last 5 of 45 syslog entries
[41][Tue Mar 19 05:08:44.280 2002][C][Switch Management:0x3e061163.304.4][User interface
session 3 user cisco@OB-session3 has been ]

[42][Tue Mar 19 05:08:44.290 2002][C][Switch Management:0x3e061163.304.4][User interface
session <4> user <cisco@OB-session4> has t]

[43][Tue Mar 19 05:08:44.290 2002][C][Switch Management:0x3e061163.304.4][User interface
session 4 user cisco@OB-session4 has been ]

[44][Tue Mar 19 05:33:13.792 2002][C][Switch Management:0x3e061163.304.4][Successful login
user cisco@OB-session3 admin 1 address U]

[45][Tue Mar 19 05:33:13.793 2002][C][Switch Management:0x3e061163.304.4][User interface
session 3 has been opened]

Display 4 devlog entries
[1][Tue Mar 19 03:10:11.057 2002][DI][Switch Log Client/0:0x3e061163.0.5][requesting
logging oper data]

[2][Tue Mar 19 03:10:11.059 2002][DI][Switch Log Client/0:0x3e061163.0.5][received,
DS_RESP_STATUS msg,id = -987127616, status = 0x]

[3][Tue Mar 19 03:10:36.797 2002][DI][Switch Log Client/0:0x3e061163.0.5][updating logging
oper data]

[4][Tue Mar 19 03:10:38.713 2002][DC][Management Server:0x3e0671163.314.6][pltdb.cc.620:
database version '2' does not match code ve]

```

Related Commands

Command	Description
fcswitch devlog	Specify logging parameters for the switch development log file.
fcswitch syslog	Specify logging parameters for the switch system log file.

show debug interface fc?

To display debug information for internal Fibre Channel (FC) interface switch ports, use the **show debug interface fc?** command.

show debug interface *fc?* [hosts | stats]

Syntax Description	<i>fc?</i>	Display debug information for the specified internal FC interface switch ports. When you type the show debug interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
	hosts	Keyword used to display FC hosts information.
	stats	Keywords used to display statistics and configuration information.

Defaults	None.
----------	-------

Command Modes	Administrator or Monitor.
---------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	The show debug interface fc? command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.
------------------	--

Examples	The following example displays debug information for the internal FC interface switch port <i>fc0</i> :
----------	---

```
[SN5428-2_PR]# show debug interface fc0
Operational Data
Interface Stat IP/Netmask          MAC          Options
-----
fc0          up
                                     type Fibre Channel
                                     OperState enabled
                                     PortID 010000
                                     WWN 200000059ba69821
                                     LinkSpeed 2Gb/s
                                     LinkState Active
                                     SyncState SyncAcquired
                                     LoginStatus LoggedIn
                                     Loopback Status Not Running
                                     MaxCredit 12
                                     DonatedToPort None
                                     RunningType f-port
                                     PendingType f-port
                                     InBandMgmt enabled
                                     SFPType NotApplicable
                                     SFPVendor N/A
                                     SFPVendorID N/A
```


show debug interface fc?

SFPPartNumber N/A
SFPRev N/A

Configuration Data										
Interface	Status	Al-fairness	Ext-credit	Fan-enable	Link-speed	Loopback-type	Mfs-bundle	Time-out	Port-type	Port-mode
fc0	enabled	disabled	0	enabled	2Gb/s	Unknown	enabled	10	f-port	

Related Commands

Command	Description
debug interface fc?	Enable IP packet tracing for the specified Gigabit Ethernet interface.

show debug interface ge?

To display IP packet trace buffer statistics and contents, use the **show debug interface ge?** command.

show debug interface ge? trace stats

show debug interface ge? trace [first *nn* | last *nn*]

show debug interface ge? trace hex [ascii] [first *nn* | last *nn*]

Syntax Description

ge?	Display IP trace information for the specified Gigabit Ethernet interface. When you type the show debug interface ge? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
trace	Display the entire trace buffer, in hex.
trace stats	Display packet trace statistics and configuration information.
first <i>nn</i>	(Optional) Display the specified number of packets from the start of the trace buffer.
last <i>nn</i>	(Optional) Display the specified number of packets from the end of the trace buffer.
trace hex	Display packet trace in hex.
ascii	(Optional) Display packet trace in hex and ASCII.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.
3.3.1	The hex and ascii keywords were added.

Usage Guidelines

To enable IP packet trace facilities for debugging Gigabit Ethernet interfaces, use the **debug interface ge?** command. The **show debug interface ge?** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.



Note

IP packet tracing must be disabled on the interface before the trace buffer can be displayed.

Examples

The following example disables IP packet tracing on the interface *ge1* and then displays the full contents of the trace buffer:

```
[SN5428-2_PR]# no debug interface ge1 trace enable

[SN5428-2_PR]# show debug interface ge1 trace
1: RX, len 60, time 0.000
0000: 01 00 0c cc cc cc 00 08 7c 3c 3d 85 00 28 aa aa
0010: 03 00 00 0c 20 04 01 00 01 00 0b 64 61 76 65 74
0020: 68 6f 00 02 00 05 81 00 03 00 05 a5 00 04 00 0a
0030: 00 08 7c 3c 3d 85 00 00 00 00 00 00
```

Related Commands

Command	Description
debug interface ge?	Enable IP packet tracing for the specified Gigabit Ethernet interface.

show debug scsirouter

To display a variety of debug information or perform specific troubleshooting activities for SCSI routing instances, use the **show debug scsirouter** command.

```
show debug scsirouter {name | all} {scsitrace | tfemapping | tfestatus}
```

```
show debug scsirouter name tfestatus verbose
```

```
show debug scsirouter name target name [lun nn [scsitrace]]
```

```
show debug scsirouter name iscsitrace [hex [ascii]] [first nn | last nn]
```

```
show debug scsirouter name iscsitrace stats
```

Syntax Description		
scsirouter <i>name</i>		The name of the SCSI routing instance.
all		Display information for all SCSI routing instances.
scsitrace		Display raw SCSI trace information for the specified SCSI routing instance or target and LUN combination.
tfemapping		Display target to physical device mapping information.
tfestatus		Display the status of the trace configuration for the specified SCSI routing instance.
verbose		Display detailed information (including management, target management and LUN management tables for all initiators) about the status of the trace configuration for the specified SCSI routing instance.
target <i>name</i>		The name of the target associated with the specified SCSI routing instance.
lun <i>nn</i>		The target LUN number.
iscsitrace		Display iSCSI trace facility output.
hex		Display iSCSI trace data in hex.
ascii		Display iSCSI trace data in hex and ASCII.
first <i>nn</i>		Display the specified number of Protocol Data Units (PDUs) from the start of the trace.
last <i>nn</i>		Display the specified number of PDUs from the end of the trace.
stats		Display iSCSI trace statistics.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.
	3.3.1	The iscsitrace , hex , ascii , first , last and stats keywords were added.

Usage Guidelines

To enable trace facilities for debugging SCSI routing instances, use the **debug scsirouter** command. The **show debug scsirouter** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

Examples

The following example displays TFE status data for the SCSI routing instance named *foo*:

```
[SN5428-2_PR]# show debug scsirouter foo tfestatus
```

The following is example output displaying the target to physical device mapping information for the SCSI routing instance named *zeus*:

```
[SN5428-2A]# show debug scsirouter zeus tfemapping
```

```
TARGET:0x0:chimaera_apps addressMapType=MAP_TYPE_LUNMAP (lun mapping)
  LUN:0x11: iSCSI2ByteLun=0x11, iScsiLun=0x0000000000000000, addressMapType=MAP_TYPE_WWNN
    Lun ID Length=8 lun ID=0x200000204819137b 00
    I: NO iSCSI Initiators Logged into target:0x0:chimaera_apps
  LUN:0x18: iSCSI2ByteLun=0x18, iScsiLun=0x0000000000000000,
addressMapType=MAP_TYPE_WWPN_LUN
    WWPN=0x22000020 0x37281505, secWWPN=0x22000020 0x37191505
    I: NO iSCSI Initiators Logged into target:0x0:chimaera_apps
  LUN:0x1f: iSCSI2ByteLun=0x1f, iScsiLun=0x0000000000000000,
addressMapType=MAP_TYPE_WWPN_LUN
    WWPN=0x22000020 0x37447b0e, secWWPN=0x22000020 0x37559b0e
    I: NO iSCSI Initiators Logged into target:0x0:chimaera_apps

TARGET:0x1:chimaera_eng addressMapType=MAP_TYPE_LUNMAP (lun mapping)
  LUN:0x11: iSCSI2ByteLun=0x11, iScsiLun=0x0000000000000000, addressMapType=MAP_TYPE_WWNN
    Lun ID Length=8 lun ID=0x20000004cf4304cd 00
    I: NO iSCSI Initiators Logged into target:0x1:chimaera_eng

TARGET:0x2:pegasus_web addressMapType=MAP_TYPE_LUNMAP (lun mapping)
  LUN:0x3: iSCSI2ByteLun=0x3, iScsiLun=0x0000000000000000,
addressMapType=MAP_TYPE_SERIAL_NUMBER
    lunSerialNumber=LS09311I0000I947ZDB5
    I: NO iSCSI Initiators Logged into target:0x2:pegasus_web

TARGET:0x3:pegasus_email addressMapType=MAP_TYPE_WWPN (target mapping)
  WorldWidePortName = 0x22000020 0x371912da, Secondary WorldWidePortName 0x22000020
0x371912da
  LUN:0x0: iSCSI2ByteLun=0x0, iScsiLun=0x0000000000000000,
addressMapType=MAP_TYPE_WWPN_LUN
    WWPN=0x22000020 0x371912da, secWWPN=0x22000020 0x372642da
    I: NO iSCSI Initiators Logged into target:0x3:pegasus_email
```

The following example of an iSCSI trace display for connections to and from the SCSI routing instance named *sr1* shows a simple login exchange. The display is formatted in hex and ASCII.

```
[SN5428-2A]# show debug scsirouter sr1 iscsitrace hex ascii
1: 10.1.50.12:1912 -> 10.1.50.100:3260, len 252, time 0.000
0000: 43 87 00 00 00 00 00 00 cb 33 39 63 35 00 00 00 00 C.....39c5....
0010: 00 01 00 00 00 01 00 00 00 00 00 01 00 00 00 00 .....
0020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0030: 54 61 72 67 65 74 4e 61 6d 65 3d 69 71 6e 2e 31 TargetName=iqn.1
0040: 39 38 37 2d 30 35 2e 63 6f 6d 2e 63 69 73 63 6f 987-05.com.cisco
0050: 3a 30 30 2e 36 62 39 35 65 39 33 64 62 62 30 39 :00.6b95e93dbb09
0060: 2e 74 31 00 4d 61 78 52 65 63 76 44 61 74 61 53 .t1.MaxRecvDataS
0070: 65 67 6d 65 6e 74 4c 65 6e 67 74 68 3d 30 78 31 egmentLength=0x1
0080: 30 30 30 30 00 49 6e 69 74 69 61 6c 52 32 54 3d 0000.InitialR2T=
0090: 4e 6f 00 49 6e 69 74 69 61 74 6f 72 4e 61 6d 65 No.InitiatorName
00a0: 3d 69 73 63 73 69 2e 63 69 73 63 6f 2e 64 61 76 =iscsi.cisco.dav
```



```

00b0: 61 76 68 6f 2d 6c 6e 78 2e 63 69 73 63 6f 2e 63  avho-lnx.cisco.c
00c0: 6f 6d 00 49 6e 69 74 69 61 74 6f 72 41 6c 69 61  om.InitiatorAlia
00d0: 73 3d 64 61 76 61 76 68 6f 2d 6c 6e 78 2e 63 69  s=davavho-lnx.ci
00e0: 73 63 6f 2e 63 6f 6d 00 53 65 73 73 69 6f 6e 54  sco.com.SessionT
00f0: 79 70 65 3d 6e 6f 72 6d 61 6c 00 00              ype=normal..

2: 10.1.50.100:3260 -> 10.1.50.12:1912, len 132, time 0.000
0000: 23 87 00 00 00 00 00 00 54 33 39 63 35 00 00 00 01  #.....T39c5....
0010: 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 01  .....
0020: 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00  .....
0030: 54 61 72 67 65 74 50 6f 72 74 61 6c 47 72 6f 75  TargetPortalGrou
0040: 70 54 61 67 3d 31 00 4d 61 78 52 65 63 76 44 61  pTag=1.MaxRecvDa
0050: 74 61 53 65 67 6d 65 6e 74 4c 65 6e 67 74 68 3d  taSegmentLength=
0060: 35 32 34 32 38 38 00 49 6e 69 74 69 61 6c 52 32  524288.InitialR2
0070: 54 3d 4e 6f 00 54 61 72 67 65 74 41 6c 69 61 73  T=No.TargetAlias
0080: 3d 74 31 00                                     =t1.

```

Related Commands

Command	Description
debug scsirouter	Enable debugging for the named SCSI routing instance.
debug scsirouter iscsitrace	Enable iSCSI trace facilities for debugging connections to and from the specified SCSI routing instance.
debug scsirouter target	Enable debugging for a specific SCSI routing instance target and LUN combination.

show devices

To display a list of devices found on the SN 5428-2 Storage Router Fibre Channel (FC) network, use the **show devices** command.

show devices [all | brief]

show devices [fc?] [lunid | serial]

show devices rediscover

Syntax Description		
all	(Optional) Keyword used to display information for all devices on all FC interfaces.	
brief	(Optional) Keyword used to limit the display to serial number information, including vendor and product, for all devices on all FC interfaces.	
<i>fc?</i>	(Optional) Limit the display to devices on the named FC interface. Valid values are fc1 through fc8. When you type the show devices fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.	
lunid	(Optional) Keyword used to limit the display to LUN information for the devices on the specified interface or all FC interfaces.	
serial	(Optional) Keyword used to limit the display to serial number information, including vendor and product, for devices on the specified interface or all FC interfaces.	
rediscover	(Optional) Begin a new discovery process on the FC network	

Defaults	None.
-----------------	-------

Command Modes	Administrator or Monitor.
----------------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Use this command to display information about all devices discovered on the named FC interface, or all FC interfaces. This information can be used when assigning targets to SCSI routing instances. The storage information includes the associated interface, WWPN, port ID, device type, LUN number, LUN ID type and LUN ID, capacity, vendor, product name, and LUN serial number.

The output of this command is limited to devices that are visible to the FC initiator interfaces (fci1 and fci2).

Use the **rediscover** keyword to clear the existing list of devices and begin a new discovery process on the FC network. Issue the **show devices** command again to display all discovered devices.

**Caution**

The **show devices rediscover** command flushes existing tables and forces a PLOGI to each device. If IP hosts are accessing a device, they will be required to wait until this process completes.

Examples

The following is example output from the **show devices rediscover** command, followed by the **show devices** command:

```
[SN5428-2A]# show devices rediscover
Fibre channel discovery kicked off!
```

```
[SN5428-2A]# show devices
Fabric Attached Devices detected
Interface WWPN                PortId  Device Type  Lun   Lunid Type        Lunid
-----
fc1        22000003be3203bc 0x101e2  Disk        0     IEEE Extended    20000003be3203bc
fc1        2200001026448a0d 0x101e1  Disk        0     IEEE Extended    2000001026448a0d
```

```
Lun Description Table
Interface WWPN                Lun   Capacity Vendor      Product      Serial
-----
fc1        22000003be3203bc 0     17GB    SEAGATE    ST207341EB  2DU0537A00006105FGJ6
fc1        2200001026448a0d 0     17GB    SEAGATE    ST207340EB  1BB00L3J0000600256DW
```

Table 12-26 describes the fields shown in the display.

Table 12-26 Description of Fields in the “show devices” Command Output

Field	Description
Interface	The FC interface associated with the storage.
WWPN	World Wide Port Name (WWPN) address.
Port Id	The port and domain ID, in hex.
Device Type	The type of physical device, for example Disk.
Lun	The physical LUN associated with the storage.
Lunid Type	The type of LUN, for example IEEE Extended.
Lunid	The unique LUN identifier, assigned when the LUN is discovered by the FC interface.
Lun Description Table	Information about the physical LUN.
Interface	The FC interface associated with the storage.
WWPN	WWPN address.
Lun	The physical LUN associated with the storage.
Capacity	The size of the storage resource, if applicable.
Vendor	The vendor of the storage resource.
Product	The product identifier.
Serial	The serial number of the storage resource.

The following is example output from the **show devices brief** command, which displays the LUN description table:

```
[SN5428-2A]# show devices brief
Lun Description Table
Interface WWPN                      Lun    Capacity Vendor      Product      Serial
-----
fc1        22000003be3203bc 0        17GB    SEAGATE    ST207341EB  2DU0537A00006105FGJ6
fc1        2200001026448a0d 0        17GB    SEAGATE    ST207340EB  1BB00L3J0000600256DW
```

The following is example output from the **show devices lunid** command:

```
[SN5428-2A]# show devices lunid
Fabric Attached Devices detected
Interface WWPN                      PortId  Device Type  Lun  Lunid Type      Lunid
-----
fc1        22000003be3203bc 0x101e2  DASD        0    IEEE Extended   20000003be3203bc
fc1        2200001026448a0d 0x101e1  DASD        0    IEEE Extended   2000001026448a0d
```

Related Commands

Command	Description
show fcswitch	Display global configuration information for storage router FC interfaces.
show interface	Display operational and configuration information about the specified interface or all interfaces.
show scsirouter	Display configuration and operational information about the named SCSI routing instance.

show diagnostics

To show that the hardware passed diagnostic tests on startup, use the **show diagnostics** command.

show diagnostics

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator or Monitor.
----------------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	The show diagnostics command is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.
-------------------------	---

Examples	The following is example output from the show diagnostics command:
-----------------	---

```
[SN5428-2A]# show diagnostics
SN5428-2 Hardware Diagnostics Passed.
```

Related Commands	Command	Description
	show tech-support	Display a variety of diagnostic information for use by Cisco Technical Support professionals.

show fcalias

To display information about aliases and their members, use the **show fcalias** command.

show fcalias {*alias-name* | **all** | **brief**}

Syntax Description	<i>alias-name</i>	The name of a specific alias entity. Only information about this alias entity will be displayed.
	all	Display information about all alias entities.
	brief	Show member information only for all alias entities.

Defaults	None.
----------	-------

Command Modes	Administrator or Monitor.
---------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

An alias is a collection of Fibre Channel (FC) devices, such as switches, initiators, storage and other SN 5428-2 Storage Routers, that can be zoned together. An alias is not a zone and cannot include a zone or another alias as a member.

Use the **show fcalias** command to display a list of members and member types for the specified alias. Use the **brief** keyword to limit the display to a list of members only.

A default alias of *iscsi* is provided that contains both initiators WWPN1 and WWPN2.

Examples

The following is example output from the **show fcalias brief** command:

```
[SN5428-2A]# show fcalias brief
Alias Name          Member value
-----
iscsi               280000048aa58710
                   290000048aa58710
labgroupa           201c00591575c229
                   201b00491585c210
webservices         2201c723591b2038
                   202100491585d220
                   202a00491585f310

3 Aliases
```


Related Commands	Command	Description
	delete fcalias	Delete the named alias or the specified alias member.
	delete zone	Delete the specified Fibre Channel zone or the specified member of the zone from the zoning database.
	delete zoneset	Delete the specified zone from the zone set or to delete the entire named zone set from the zoning database.
	fcalias	Create an alias entity for use in Fibre Channel zoning.
	fcalias member	Add the specified member to the named alias.
	show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
	show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
	zone	Create a Fibre Channel fabric zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset enable	Activate a zone set.

show fcip

To display configuration information and operational statistics related to the named FCIP instance or all instances, use the **show fcip** command.

```
show fcip {name | all} [from {filename | bootconfig | runningconfig}]  
  
show fcip {name | all} [brief | stats]
```

Syntax Description

<i>name</i>	The name of the FCIP instance. Valid names are <i>fcip1</i> and <i>fcip2</i> .
all	Display the requested information for all FCIP instances.
from <i>filename</i>	(Optional) The name of the saved configuration file containing the specified FCIP instance information. This file must exist in the <i>savedconfig</i> directory.
from bootconfig	(Optional) Display the requested configuration information from the persistent saved configuration.
from runningconfig	(Optional) Display the requested configuration information from the currently running configuration.
brief	(Optional) Display status and brief configuration information.
stats	(Optional) Display accumulated operational information for the FCIP instance. This display shows statistics accumulated since the named FCIP instance became active or statistics were last cleared, whichever is more recent.

Defaults

When no **from** parameters are specified, the information displayed is from the currently running configuration.

Command Modes

Administrator or Monitor

Command History

Release	Modification
3.3.1	This command was introduced.

Usage Guidelines

The **show fcip** command displays the current link state, connection state, Fibre Channel firmware version and state, packet trace mask and mailbox trace state. This command also show protocol specific connection information, such as current TCP window sizes or the raw IP flow control and error statistics.

Use the **stats** keyword to display accumulated operational information of the specified FCIP instance. Operational statistics include the number of Fibre Channel link changes, network connects, asynchronous events, and Fibre Channel errors.

Examples

The following is example output from the show fcip command. In this example, the FCIP instance is configured to use a raw IP connection.

```
[SN5428-2A]# show fcip fcip1
Instance  Device I/F  Network I/F
-----
fcip1     fci1      ge1 10.1.0.16

Description
-----
Accessing SAN island 5

Destination  Mode      IpAddress      IsConnected
-----
dest1        raw       10.2.70.110    TRUE

LinkState
-----
UP

fcip1 Trace Status
-----
pktTraceMask      On, mask 0xffff
mboxTracing        On
mboxCmdCount       0

fcip1 Connection Information
-----
idlePingDelay      60
txAck              0x38
txSeq              0x39
rxAck              0x38
rxSeq              0x38
peerNeedsAck       0x0
WackQ              0x0, 0xca69d08
WackQCnt           0x0
WackQExtra         0x0
frOut              0x0
frOutHiWater       0x400
bcOut              0x0
bcOutHiWater       0x200000
burstOut           0x0
burstOutHiWater    0x200000
outFlowCtrlQ       0x0, 0x0
frIn               0x0
frInHiWater        0x2b0
inFlowCtrlQ        0x0, 0x0
blockMaxSize       0x0
oosPktQ            0x0, 0x0
ipProtocol          0x4
reXmitCnt           0x4
reXmitMaxTO        0x30
reXmitTimeOutIncr   0x0
reXmitInitialTimeOut 0x0
reXmitTotalTimeOut  0x0
    192ms 256ms 384ms 768ms
```


The following is example output from the show fcip command. In this example, the FCIP instance is configured to use a TCP server connection.

```
[SN5428-2A]# show fcip fcip2

Instance  Device I/F  Network I/F
-----  -
fcip2    fci2      ge2  10.1.40.42

Description
-----
Testing SAN

Destination  LocalMode  IPAddress      IsConnected
-----
dest2        tcpserver  10.2.50.51     TRUE

LinkState
-----
UP

fcip1 Trace Status
-----
pktTraceMask          On, mask 0xffff
mboxTracing            On
mboxCmdCount           0

fcip1 Connection Information
-----
idlePingDelay          60
tcpPort                 3225
rxTcpWindowSize        262144
maxRxTcpWindowSize     262144
txTcpWindowSize        262080
txTcpCongestionWindowSize 268800
maxTxTcpWindowSize     262144
frIn                    0
frInHiWater            688
```

Table 12-27 describes the fields in the display:

Table 12-27 Description of Fields in the “show fcip” Command Output

Field	Description
Instance	The name of the FCIP instance.
Device I/F	The internal Fibre Channel interface associated with this FCIP instance.
Network I/F	The Gigabit Ethernet interface and IP address associated with this FCIP instance.
Description	The FCIP instance description, if any.
Destination	The name of the FCIP peer destination.
Mode	The connection protocol type used by this FCIP instance.
IpAddress	The IP address of the peer FCIP instance.
IsConnected	The state of the connection between this FCIP instance and its peer.
LinkState	The state of the link.

Table 12-27 Description of Fields in the “show fcip” Command Output (continued)

Field	Description
Trace Status	Operational information about FCIP traces.
pktTraceMask	The trace mask.
mboxTracing	Indicates if tracing is turned on for the FCIP instance.
mboxCmdCount	The number of commands that have been traced.
Connection Information	Configuration and operational information about the FCIP instance connection to the peer.
idlePingDelay	The number of seconds before a keep-alive packet is sent across an idle connection.
txAck	The number of the last transmitted acknowledgement (ACK).
txSeq	The last transmitted sequence number.
rxAck	The number of the last received ACK.
rxSeq	The last received sequence number.
peerNeedsAck	The current number of unacknowledged frames.
WackQ	The head and tail pointers of non-acknowledged packets.
WackQCnt	The total number of packets waiting for ACKs.
WackQExtra	The number of packets acknowledged but not returned from the Gigabit Ethernet driver.
frOut	The number of Fibre Channel (FC) frames that have been transmitted on the Gigabit Ethernet interface, but not yet acknowledged.
frOutHiWater	The maximum number of frames that can be outstanding on a raw IP connection.
bcOut	The total number of FC octets transmitted on the Gigabit Ethernet interface, but not yet acknowledged.
bcOutHiWater	The maximum number of bytes that can be outstanding on a raw IP connection.
burstOut	The number of bytes given to the Gigabit Ethernet interface, but not returned.
burstOutHiWater	The maximum number of bytes that can be transmitted on a raw IP connection.
outFlowCtrlQ	The head and tail pointers of queued packets waiting on Gigabit Ethernet transmit flow control.
frIn	The number of FC frames given to the FC interface.
frInHiWater	The maximum number of frames, received from a raw IP connection, that can be sent to the FC interface.
inFlowCtrlQ	The head and tail pointers of queued packets waiting on FC transmit flow control.
blockMaxSize	The maximum block size, if blocking FC frames.
oosPktQ	The head and tail pointers of packets received out-of-sequence, waiting for in- sequence packets.

Table 12-27 Description of Fields in the “show fcip” Command Output (continued)

Field	Description
ipProtocol	The value of the IP protocol used in the IP header.
reXmitCnt	The maximum number of times a packet can be retransmitted, before it is discarded.
reXmitMaxTO	The maximum amount of time, in ticks, that can be used for any one retransmission, before the packet is discarded.
reXmitTimeOutIncr	The amount of time, in ticks, to add to a packet's time out value before retransmitting the packet
reXmitInitialTimeOut	The initial amount of time, in ticks, to delay before retransmitting a packet.
reXmitTotalTimeOut	The maximum amount of time, in ticks, that a packet is kept alive, before it is discarded.
Millisecond values	The retransmission intervals, based on the error recovery algorithm.
tcpPort	The TCP port number. The TCP server listens to this port; the TCP client connects to this port.
rxTcpWindowSize	The current maximum number of outstanding bytes that can be received on a TCP connection.
maxRxTcpWindowSize	The configured maximum number of outstanding bytes that can be received on a TCP connection.
txTcpWindowSize	The configured maximum number of outstanding bytes that can be transmitted on a TCP connection.
txTcpCongestionWindowSize	The size of the congestion controlled window, in bytes.
maxTxTcpWindowSize	The current maximum number of outstanding bytes that can be transmitted on a TCP connection. This is the largest window that the peer has offered.

The following is example output from the **show fcip brief** command:

```
[SN5428-2A]# show fcip fcip1 brief
Instance  Device I/F  Network I/F
-----
fcip1     fci1      ge1 10.1.0.16

Description
-----
Accessing SAN island 5

Destination  Mode      IpAddress      IsConnected
-----
dest1        tcpclient  10.2.70.110    TRUE

LinkState
-----
UP
```


The following is example output from the **show fcip stats** command:

```
[SN5428-2A]# show fcip all stats
fcip1
-----
Mode                               tcpclient
Destination Address                 10.1.40.170
Connected                           Yes

fcip1 Stats
-----
Link up events                      1
Link down events                    0
Connect events                      1
Network connections established     1
Network flow controlled             1
fcip2
-----
Mode                               raw
Destination Address                 10.1.50.53
Connected                           Yes

fcip2 Stats
-----
Link up events                      1
Link down events                    0
Connect events                      1
Network connections established     1
Network flow controlled             1
```

Related Commands

Command	Description
clear counters fcip	Reset accumulated operational statistics for the specified SCSI routing instance.
fcip	Create an FCIP instance.
fcip description	Add user-defined identification information to the named FCIP instance.
fcip destination config	Configure operational parameters for the named FCIP instance.
fcip destination raw	Add a peer destination to the named FCIP instance, with a connection type of raw IP.
fcip destination tcpclient	Add a peer destination to the named FCIP instance, with a connection type of TCP/IP. The named FCIP instance initiates the TCP connection.
fcip destination tcpserver	Add a peer destination to the named FCIP instance, with a connection type of TCP/IP. The named FCIP instance listens for the TCP connection from the named destination.
fcip networkif	Assign a Gigabit Ethernet interface and IP address to the named FCIP instance.
restore fcip	Restore the named SCSI routing instance from the named configuration file.
save fcip	Save configuration information for the named FCIP instance.

show fcswitch

To display global configuration information for SN 5428-2 Storage Router Fibre Channel (FC) interfaces, use the **show fcswitch** command.

show fcswitch

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines This command displays global configuration information, including error detect timeout value and resource allocation timeout value, for all FC interfaces.

Examples The following example displays global configuration information for all FC interfaces:

```
SN5428-2A]# show fcswitch
Global attributes                               Value
-----
Domain ID                                     1
Domain ID lock                               disabled
Active Zoneset                               None
Zoning Merge                                SW2
Zoning Default                               All
Zoning Autosave                             enabled
Distributed Services timeout (dstov)         5000
Fabric Services timeout (fstov)              1000
Error Detect timeout (edtov)                  2000
Resource Allocation timeout (ratov)           10000
Buffer to Buffer Credit (interop)             12
Initiator WWPN1                              280000023e081120
Initiator WWPN2                              290000023e081120
```


Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	delete zone	Delete the specified Fibre Channel zone or the specified member of the zone from the zoning database.
	delete zoneset	Delete the specified zone from the zone set or delete the entire named zone set from the zoning database.
	fcswitch domainid	Set the domain ID for the storage router, to be used for FC switched fabric zoning.
	fcswitch dstov	Specify the amount of time the storage router is to wait for Fibre Channel Distributed Services.
	fcswitch edtov	Specify an error detect timeout value for all Fibre Channel interfaces.
	fcswitch enable	Enable all FC interfaces.
	fcswitch fstov	Specify the fabric stability timeout value.
	fcswitch interop-credit	Set the data buffer credit capacity for all FC ports.
	fcswitch ratov	Specify a Fibre Channel resource allocation timeout value for the storage router.
	fcswitch zoning autosave	Enable the SN 5428-2 Storage Router to save zoning changes received from switches in the fabric.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	fcswitch zoning merge	Set zoning merge compliance.
	show debug fcswitch	Display internal Fibre Channel interface parameters.
	show interface	Display operational and configuration information for the specified interface or all interfaces.
	show fcswitch eport	Display FSPF protocol information.
	show fcswitch fabric	Display information about the Fibre Channel fabric.
	show fcswitch global-nameserver	Display the Fibre Channel fabric nameserver database.
	show fcswitch linkstate	Display information about the storage router link state database.
	show fcswitch nameserver	Display the local Fibre Channel nameserver database.
	show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
	show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
	zone	Create a Fibre Channel fabric zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset enable	Activate a zone set.

show fcswitch eport

To display Fabric Shortest Path First (FSPF) protocol information for the Fibre Channel (FC) fabric, use the **show fcswitch eport** command.

show fcswitch eport {all | brief}

Syntax Description	all	Display complete FSPF information for all switches in the fabric.
	brief	Display abbreviated FSPF information for all switches in the fabric.

Defaults	None.
----------	-------

Command Modes	Administrator or Monitor.
---------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to show FSPF information for all switches in the fabric.
------------------	---

Examples The following is example output from the **show fcswitch eport brief** command:

```
[SN5428-2A]# show fcswitch eport brief
Domain Id Node WWN          Source Port Hops Cost   Age    Incarnation Links
-----
99          100000059ba69821  255          0     0    580    80000024    0

1 entry found
```

[Table 12-28](#) describes the fields in the display:

Table 12-28 Description of Fields in the “show fcswitch eport brief” Command Output

Field	Description
Domain Id	The domain ID of the SN 5428-2 Storage Router or switch in the fabric.
Node WWN	The node’s World Wide Name.
Source Port	The node’s source port number.
Hops	The number of hops to the specified node.
Cost	The calculated cost.
Age	The age of the entry.

Table 12-28 Description of Fields in the “show fcswitch eport brief” Command Output (continued)

Field	Description
Incarnation	The link state incarnation number.
Links	The number of links associated with this node.

Related Commands

Command	Description
clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
fcswitch domainid	Set the domain ID for the storage router, to be used for FC switched fabric zoning.
fcswitch enable	Enable all FC interfaces.
restore fcswitch	Restore Fibre Channel configuration information from the named configuration file.
save fcswitch	Save all Fibre Channel configuration, including global configuration settings and zoning information.
show debug fcswitch	Display internal Fibre Channel interface parameters.
show fcswitch	Display global configuration information for storage router FC interfaces.
show fcswitch fabric	Display information about the Fibre Channel fabric.
show fcswitch linkstate	Display information about the storage router link state database.

show fcswitch fabric

To display information about the Fibre Channel (FC) fabric, use the **show fcswitch fabric** command.

show fcswitch fabric {all | brief}

Syntax Description	all	Display complete information for all domains in the fabric.
	brief	Display abbreviated information for all domains in the fabric.

Defaults	None.
----------	-------

Command Modes	Administrator or Monitor.
---------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to display all nodes available in the fabric, along with associated domain ID and node ID.
------------------	---

Examples	The following is output from the show fcswitch fabric brief command:
----------	---

```
[SN5428-2A]# show fcswitch fabric brief
Domain Id Node Id WWN
-----
99          fffc4f  100000059ba69821
```


Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	delete zone	Delete the specified Fibre Channel zone or the specified member of the zone from the zoning database.
	delete zoneset	Delete the specified zone from the zone set or delete the entire named zone set from the zoning database.
	fcswitch domainid	Set the domain ID for the storage router, to be used for FC switched fabric zoning.
	fcswitch dstov	Specify the amount of time the storage router is to wait for Fibre Channel Distributed Services.
	fcswitch edtov	Specify an error detect timeout value for all Fibre Channel interfaces.
	fcswitch enable	Enable all FC interfaces.
	fcswitch fstov	Specify the fabric stability timeout value.
	fcswitch interop-credit	Set the data buffer credit capacity for all FC ports.
	fcswitch ratov	Specify a Fibre Channel resource allocation timeout value for the storage router.
	fcswitch zoning autosave	Enable the SN 5428-2 Storage Router to save zoning changes received from switches in the fabric.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	fcswitch zoning merge	Set zoning merge compliance.
	show debug fcswitch	Display internal Fibre Channel interface parameters.
	show interface	Display operational and configuration information for the specified interface or all interfaces.
	show fcswitch	Display global configuration information for storage router FC interfaces.
	show fcswitch eport	Display FSPF protocol information.
	show fcswitch global-nameserver	Display the Fibre Channel fabric nameserver database.
	show fcswitch linkstate	Display information about the storage router link state database.
	show fcswitch nameserver	Display the local Fibre Channel nameserver database.
	show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
	show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
	zone	Create a Fibre Channel fabric zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset enable	Activate a zone set.

show fcswitch global-nameserver

To display the Fibre Channel (FC) fabric nameserver database, use the **show fcswitch global-nameserver** command.

```
show fcswitch global-nameserver {all | brief}
```

Syntax Description	all	Display the fabric nameserver database.
	brief	Display abbreviated information from the fabric nameserver database.

Defaults	None.
----------	-------

Command Modes	Administrator or Monitor.
---------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

All devices in a fabric are assigned a unique 24-bit public address by the fabric. The fabric also maintains a database of all the devices and their addresses. The database is called the fabric *nameserver*, and is used by host connections to determine the devices that they can communicate with.

Use this command to display the fabric nameserver database.

Examples

The following is example output from the **show fcswitch global-nameserver brief** command. A table of information, including domain ID, displays for each switch in the fabric.

```
[SN5428-2A]# show fcswitch global-nameserver brief
domainId = 1

Port Id Port Type Port Number      Port WWN              Port IP Address
-----
010000 N          0          280000054227b610    00000000
0105c1 NL          5          21000003be64e2aa    00000000
0105c2 NL          5          21000003be64e2ac    00000000
0105c3 NL          5          21000003be3a6dc1    00000000
0105c4 NL          5          21000003be64e03b    00000000
0105c5 NL          5          21000003be64e25c    00000000
0105c6 NL          5          21000003be64e252    00000000
010f00 N          15         290000054227b610    00000000

8 entries found for domain id 1
```



```
domainId = 239
```

Port Id	Port Type	Port Number	Port WWN	Port IP Address
ef0000	N	Unknown	280000012c061100	00000000
ef02ef	NL	Unknown	210000d07a031e24	00000000
ef04d1	NL	Unknown	21000003be64e2a5	00000000
ef04d2	NL	Unknown	21000003be64e22e	00000000
ef04d3	NL	Unknown	21000003be64e2a2	00000000
ef04d4	NL	Unknown	21000003be64e225	00000000
ef04d5	NL	Unknown	21000003be64e206	00000000
ef04d6	NL	Unknown	21000003be64e220	00000000
ef04d9	NL	Unknown	21000003be64e22a	00000000
ef04da	NL	Unknown	21000003be64e2a8	00000000
ef04dc	NL	Unknown	2100001026b4105d	00000000
ef04e0	NL	Unknown	2100001026b4087a	00000000
ef0f00	N	Unknown	290000021c061100	00000000

```
13 entries found for domain id 239
```


Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	delete zone	Delete the specified Fibre Channel zone or the specified member of the zone from the zoning database.
	delete zoneset	Delete the specified zone from the zone set or delete the entire named zone set from the zoning database.
	fcswitch domainid	Set the domain ID for the storage router, to be used for FC switched fabric zoning.
	fcswitch dstov	Specify the amount of time the storage router is to wait for Fibre Channel Distributed Services.
	fcswitch edtov	Specify an error detect timeout value for all Fibre Channel interfaces.
	fcswitch enable	Enable all FC interfaces.
	fcswitch fstov	Specify the fabric stability timeout value.
	fcswitch interop-credit	Set the data buffer credit capacity for all FC ports.
	fcswitch ratov	Specify a Fibre Channel resource allocation timeout value for the storage router.
	fcswitch zoning autosave	Enable the SN 5428-2 Storage Router to save zoning changes received from switches in the fabric.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	fcswitch zoning merge	Set zoning merge compliance.
	show debug fcswitch	Display internal Fibre Channel interface parameters.
	show interface	Display operational and configuration information for the specified interface or all interfaces.
	show fcswitch	Display global configuration information for storage router FC interfaces.
	show fcswitch eport	Display FSPF protocol information.
	show fcswitch fabric	Display information about the Fibre Channel fabric.
	show fcswitch linkstate	Display information about the storage router link state database.
	show fcswitch nameserver	Display the local Fibre Channel nameserver database.
	show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
	show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
	zone	Create a Fibre Channel fabric zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset enable	Activate a zone set.

show fcswitch linkstate

To display information about the SN 5428-2 Storage Router link state database, use the **show fcswitch linkstate** command.

show fcswitch linkstate database

Syntax Description	database	Display current link information for all Fibre Channel (FC) ports.
--------------------	----------	--

Defaults	None.
----------	-------

Command Modes	Administrator or Monitor.
---------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to display link state information for each FC interface, including the initiator interfaces (fc0 and fc15).
------------------	--

Examples	The following is output from the show fcswitch linkstate command:
----------	--

```
[SN5428-2A]# show fcswitch linkstate database
Local Node WWN      100000059ba69821
Local Port          15
Local Port WWN      200f00059ba69821
Remote Node WWN     100000059ba69820
Remote Port         ffffffff
Remote Port WWN     290000059ba69820
Remote Agent Address 00000000
Remote Agent Type    0
Remote Agent Port    0
Remote Unit Type     Unknown
Remote Connection Id 0000ef

Local Node WWN      100000059ba69821
Local Port          0
Local Port WWN      200000059ba69821
Remote Node WWN     100000059ba69820
Remote Port         ffffffff
Remote Port WWN     280000059ba69820
Remote Agent Address 00000000
Remote Agent Type    0
Remote Agent Port    0
Remote Unit Type     Unknown
Remote Connection Id 4f0000
```


show fcswitch linkstate

```

Local Node WWN      100000059ba69821
Local Port          1
Local Port WWN      200100059ba69821
Remote Node WWN     2000002037559b0e
Remote Port         ffffffff
Remote Port WWN     2200002037559b0e
Remote Agent Address 00000000
Remote Agent Type   0
Remote Agent Port   0
Remote Unit Type    Unknown
Remote Connection Id 0000e1

```

```

Local Node WWN      100000059ba69821
Local Port          1
Local Port WWN      200100059ba69821
Remote Node WWN     20000004cf4304cd
Remote Port         ffffffff
Remote Port WWN     22000004cf4304cd
Remote Agent Address 00000000
Remote Agent Type   0
Remote Agent Port   0
Remote Unit Type    Unknown
Remote Connection Id 0000e2

```

```

Local Node WWN      100000059ba69821
Local Port          15
Local Port WWN      200f00059ba69821
Remote Node WWN     100000059ba69820
Remote Port         ffffffff
Remote Port WWN     290000059ba69820
Remote Agent Address 00000000
Remote Agent Type   0
Remote Agent Port   0
Remote Unit Type    Unknown
Remote Connection Id 4f0f00

```

5 entries found

Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	delete zone	Delete the specified Fibre Channel zone or the specified member of the zone from the zoning database.
	delete zoneset	Delete the specified zone from the zone set or delete the entire named zone set from the zoning database.
	fcswitch domainid	Set the domain ID for the storage router, to be used for FC switched fabric zoning.
	fcswitch dstov	Specify the amount of time the storage router is to wait for Fibre Channel Distributed Services.
	fcswitch edtov	Specify an error detect timeout value for all Fibre Channel interfaces.
	fcswitch enable	Enable all FC interfaces.
	fcswitch fstov	Specify the fabric stability timeout value.
	fcswitch interop-credit	Set the data buffer credit capacity for all FC ports.
	fcswitch ratov	Specify a Fibre Channel resource allocation timeout value for the storage router.
	fcswitch zoning autosave	Enable the SN 5428-2 Storage Router to save zoning changes received from switches in the fabric.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	fcswitch zoning merge	Set zoning merge compliance.
	show debug fcswitch	Display internal Fibre Channel interface parameters.
	show interface	Display operational and configuration information for the specified interface or all interfaces.
	show fcswitch	Display global configuration information for storage router FC interfaces.
	show fcswitch eport	Display FSPF protocol information.
	show fcswitch fabric	Display information about the Fibre Channel fabric.
	show fcswitch global-nameserver	Display the Fibre Channel fabric nameserver database.
	show fcswitch nameserver	Display the local Fibre Channel nameserver database.
	show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
	show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
	zone	Create a Fibre Channel fabric zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset enable	Activate a zone set.

show fcswitch nameserver

To display the local Fibre Channel (FC) nameserver database, use the **show fcswitch nameserver** command.

show fcswitch nameserver {all | brief}

Syntax Description	all	Display the local fabric nameserver database.
	brief	Display abbreviated information from the local fabric nameserver database.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

All devices in a fabric are assigned a unique 24-bit public address by the fabric. The fabric also maintains a database of all the devices and their addresses. The database is called the fabric *nameserver*, and is used by host connections to determine the devices that they can communicate with.

Use this command to display the local fabric nameserver database.

Examples

The following is example output from the **show fcswitch nameserver brief** command:

```
[SN5428-2A]# show fcswitch nameserver brief
Port Id Port Type Port Number      Port WWN          Port IP Address
-----
4e0000 N          0          280000048aa58710  00000000
4e01d1 NL          1          2200001026448a0d  00000000
4e01d2 NL          1          22000003be3203bc  00000000
4e0e00 N          15         290000048aa58710  00000000

4 entries found
```


Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	delete zone	Delete the specified Fibre Channel zone or the specified member of the zone from the zoning database.
	delete zoneset	Delete the specified zone from the zone set or delete the entire named zone set from the zoning database.
	fcswitch domainid	Set the domain ID for the storage router, to be used for FC switched fabric zoning.
	fcswitch dstov	Specify the amount of time the storage router is to wait for Fibre Channel Distributed Services.
	fcswitch edtov	Specify an error detect timeout value for all Fibre Channel interfaces.
	fcswitch enable	Enable all FC interfaces.
	fcswitch fstov	Specify the fabric stability timeout value.
	fcswitch interop-credit	Set the data buffer credit capacity for all FC ports.
	fcswitch ratov	Specify a Fibre Channel resource allocation timeout value for the storage router.
	fcswitch zoning autosave	Enable the SN 5428-2 Storage Router to save zoning changes received from switches in the fabric.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	fcswitch zoning merge	Set zoning merge compliance.
	show debug fcswitch	Display internal Fibre Channel interface parameters.
	show interface	Display operational and configuration information for the specified interface or all interfaces.
	show fcswitch	Display global configuration information for storage router FC interfaces.
	show fcswitch eport	Display FSPF protocol information.
	show fcswitch fabric	Display information about the Fibre Channel fabric.
	show fcswitch global-nameserver	Display the Fibre Channel fabric nameserver database.
	show fcswitch linkstate	Display information about the storage router link state database.
	show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
	show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
	zone	Create a Fibre Channel fabric zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset enable	Activate a zone set.

show ha

To display HA configuration and status information and HA statistics for the SN 5428-2 Storage Router or selected applications and SCSI routing instances running in the HA environment, use the **show ha** command.

```
show ha all

show ha app {all | list} stats

show ha app nn {stats | failover list}

show ha node stats
```

Syntax Description	all	Display brief HA status and configuration information.
	app all stats	Show HA statistics for all applications.
	app list stats	Display a list of HA applications and brief HA statistics. This list includes application numbers.
	app nn stats	Display HA statistics for the specified application number.
	app nn failover list	Display the failover list for the specified SCSI routing instance.
	node stats	Generate a display of HA statistics for the storage router.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Use this command to help determine if there are communications problems within the high availability cluster. The **show ha all** command displays the state of the management and HA interfaces, and the status of the intelligent automatic failover feature.

To display statistics about all applications, issue this command:

```
[SN5428-2A]# show ha app all stats
```

To display a list of SCSI routing instances and other HA applications, with their creation dates and last time of fail over, issue this command:

```
[SN5428-2A]# show ha app list stats
```


Examples

The following is example output from the **show ha** command, using the **app list** keywords to display a list of applications and SCSI routing instances:

```
[SN5428-2A]# show ha app list stats

-----HA APPLICATION LIST-----

Type = cluster                      Created = Tue Mar 19 17:08:02 CDT 2002
  (Number 01)  cluster/myCluster    Created = Tue Mar 19 17:08:03 CDT 2002
                                     Activated = Tue Mar 19 17:08:03 CDT 2002
                                     Last Failover = no failover yet

Type = scsirouter                  Created = Tue Mar 19 17:08:02 CDT 2002
  (Number 02)  scsirouter/myScsi1   Created = Wed Mar 20 16:36:02 CDT 2002
                                     Activated = Wed Mar 20 16:36:07 CDT 2002
                                     Last Failover = no failover yet
  (Number 03)  scsirouter/myScsi1   Created = Wed Mar 20 18:20:14 CDT 2002
                                     Activated = Thu Mar 21 07:45:01 CDT 2002
                                     Last Failover = Thu Mar 21 11:15:33 CDT 2002

-----
```

Table 12-29 describes the significant fields shown in the display.

Table 12-29 Description of Fields in the “show ha” Command Output

Field	Description
Type	The type of HA application or service.
Created	The date and time that the application or service type was created.
Number	The HA application or service number. This number is used in the show ha command with the app keyword to display information about that specific application or service.
Created	The date and time that the specific application or service was created.
Activated	The date and time that the specific application or service became active.
Last Failover	The date and time that the specific application or service last failed over.

The following is example output from the **show ha** command, using the **app nn stats** keyword and parameter to display operational statistics about the SCSI routing instance named *foo*:

```
[SN5428-2A]# show ha app 02 stats

-----HA APPLICATION Number 2-----
Application Name = scsirouter/foo
Type = scsirouter      Master Specifics:      DataBase:
AppId = 0759e950       Node Id = 0042f1a7      ID = 597099c8
State = Master         Preferred Slave = No    Status = Up to Date
Eligibility = 00000003 Permanent Master = No   Last Update =
                                     Mon Apr 8 21:03:55 GMT 2002
                                     Pndg ID = 00000000
                                     Prev ID = 7b1d240d
```



```
show ha
```

```
HA Message Transmission Summary:
Total = 00000005      Multicasts = 00000002      Unicasts = 00000003
HA Message Reception Summary:
Total = 00000004
```

```
-----Message Breakdown-----
      Message Types Received      Message Types Transmitted
Master Requests = 00000002      Master Requests = 00000001
Master Acks = 00000001          Master Acks = 00000002
Elections = 00000001            Elections = 00000001
Refusals = 00000000             Refusals = 00000000
Conflicts = 00000000            Conflicts = 00000000
Resolves = 00000000             Resolves = 00000000
Quits = 00000000                Quits = 00000000
Resignations = 00000000         Resignations = 00000001
Doas = 00000000                 Doas = 00000000
```

Table 12-30 describes the significant fields shown in the display.

Table 12-30 Description of Fields in the “show ha app” Command Output

Field	Description
Application Name	The complete name of the HA application. The syntax is <i>application-type/application name</i> .
Type	The HA application type.
AppId	The HA application identification number.
State	The state of the HA application.
Eligibility	The failover eligibility indicator.
Master Specifics: Node Id	The ID of the node that is currently running the HA application.
Preferred Slave	Indicates if the storage router is the first node on the failover list for this HA application.
Permanent Master	Indicates if the storage router is defined as the primary for the HA application.
Database: ID	The ID of the internal database entry associated with this HA application.
Status	Indicates if the database is current or if there is an outstanding configuration update pending.
Last Update	The date and time of the last update to this HA application.
HA Message Transmission Summary	The number of HA messages that have been transmitted by this application. The Total value is the sum of the Broadcasts and the Unicasts.

Table 12-30 Description of Fields in the “show ha app” Command Output (continued)

Field	Description
HA Message Reception Summary	The total number of HA messages received by this application.
Message Breakdown	<p>The number of each type of HA message that has been received and transmitted by this HA application. The following are HA message types:</p> <ul style="list-style-type: none"> • Master Requests • Master Acks • Elections • Refusals • Conflicts • Resolves • Quits • Resignations • Doas

Related Commands

Command	Description
failover eligibility	Enable intelligent automatic failover for all SCSI routing instances running on the storage router.
interface ha ip-address	Specify the HA interface IP address and subnet mask.
setup cluster	Change the configuration of the high availability environment.
show cluster	Display cluster-related operational statistics, including heartbeat information.
show interface	Display operational and configuration information for the specified interface or all interfaces.

show interface

To display operational characteristics and statistics for interfaces configured for the SN 5428-2 Storage Router, use the **show interface** command. Statistics are cumulative since the last time the system was started.

```
show interface

show interface brief [expression]

show interface {if-name | all} [stats]

show interface if-name iscsilogins
```

Syntax	Description
brief	Show basic operational characteristics for all interfaces, including status, IP address, and selected options.
<i>expression</i>	(Optional) Limit the display to selected options that matches this expression.
<i>if-name</i>	Show basic operational characteristics and configuration data for the specified interface. Valid interface names are listed in Table 12-31 .
all	Display operational and configuration data for all interfaces.
stats	(Optional) Show operational statistics, such as number of input and output packets, for the specified interface.
iscsilogins	Show iSCSI host logins for the specified interface. This keyword is only valid when the storage router is deployed for transparent SCSI routing.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

- Usage Guidelines**
- Use the **show interface** command with no parameters to display the basic operational characteristics and configuration data for all interfaces.
 - Use the **show interface brief** command to display basic operational characteristics for each of the interfaces. This display includes status (up or down) information for the interface and selected operational options such as type of interface, MTU size, and speed. Use the *expression* argument to limit the display to options that match the expression.

- Use the **show interface *if-name* stats** command to display operational statistics related to the specified interface. This information can include packets received and transmitted, collisions, octets, multicast packets, dropped and unsupported protocol, exception status IOCBs (such as LIP reset aborts, port unavailable or logged out, DMA errors, port configuration changed, command timeout, data overrun, write or read data underrun, and queue full), Fibre Channel (FC) errors, and other general events.

Table 12-31 Valid Interface Names

Interface Name	Description
fc?	The FC interface, for example fc1 or fc5.
fci?	The internal FC interface, for example fci1 or fci2.
ge?	The Gigabit Ethernet interface, for example, ge1 or ge2.
ha	The high availability interface.
mgmt	The management interface.

Examples

The following is example output from the **show interface** command:

```
[SN5428-2A]# show interface
```

```
Operational Data
```

Interface	Stat	IP/Netmask	MAC	Options
lo0	up	127.0.0.1/ff000000	000000000000	type Loopback mtu 32768 speed 0 flags UP LOOPBK RUNNING MLTCST
mgmt	up	10.1.10.244/ffffff00	00023d070cc0	type Ethernet mtu 1500 speed 100000000 flags UP BRDCST RUNNING MLTCST
ha	up	10.1.20.56/ffffff00	00023d070cc1	type Ethernet mtu 1500 speed 100000000 flags UP BRDCST RUNNING MLTCST
fei2	up	2.0.0.1/ffffff00	00065338bc22	type Ethernet mtu 1500 speed 100000000 flags UP BRDCST RUNNING MLTCST
fc0	up			type Fibre Channel OperState enabled PortID 010000 WWN 200000059ba69821 LinkSpeed 2Gb/s LinkState Active SyncState SyncAcquired LoginStatus LoggedIn Loopback Status Not Running MaxCredit 12 DonatedToPort None RunningType f-port PendingType f-port InBandMgmt enabled SFPTType NotApplicable SFPVendor N/A SFPVendorID N/A SFPPartNumber N/A SFPRev N/A

■ show interface

fc1	up	type Fibre Channel OperState enabled PortID 010100 WWN 200100c0aa00bc30 LinkSpeed 1Gb/s LinkState Active SyncState SyncAcquired LoginStatus LoggedIn Loopback Status Not Running MaxCredit 12 DonatedToPort None RunningType fl-port PendingType gl-port InBandMgmt enabled SFPTType 100-M5-SN-1 SFPVendor PICOLIGHT SFPVendorID 850400 SFPPartNumber PL-XPL-00-S23-00 SFPRev
fc2	down	type Fibre Channel OperState disabled PortID 010200 WWN 200200c0cc00ac30 LinkSpeed auto LinkState Inactive SyncState SyncLost LoginStatus NotLoggedIn Loopback Status Not Running MaxCredit 12 DonatedToPort None RunningType Unknown PendingType gl-port InBandMgmt enabled SFPTType NotInstalled SFPVendor Unknown SFPVendorID 0 SFPPartNumber Unknown SFPRev 0
fc3	down	type Fibre Channel OperState disabled PortID 010300 WWN 200300c0cc00ac30 LinkSpeed auto LinkState Inactive SyncState SyncLost LoginStatus NotLoggedIn Loopback Status Not Running MaxCredit 12 DonatedToPort None RunningType Unknown PendingType gl-port InBandMgmt enabled SFPTType NotInstalled SFPVendor Unknown SFPVendorID 0 SFPPartNumber Unknown SFPRev 0
fc4	down	type Fibre Channel OperState disabled PortID 010400 WWN 200400c0bb00ac30 LinkSpeed auto LinkState Inactive SyncState SyncLost

fc5 down

```

LoginStatus NotLoggedIn
Loopback Status Not Running
MaxCredit 12
DonatedToPort None
RunningType Unknown
PendingType gl-port
InBandMgmt enabled
SFPTType NotInstalled
SFPVendor Unknown
SFPVendorID 0
SFPPartNumber Unknown
SFPRev 0
type Fibre Channel
OperState disabled
PortID 010500
WWN 200500c0dd00bc30
LinkSpeed auto
LinkState Inactive
SyncState SyncLost
LoginStatus NotLoggedIn
Loopback Status Not Running
MaxCredit 12
DonatedToPort None
RunningType Unknown
PendingType fl-port
InBandMgmt enabled
SFPTType NotInstalled
SFPVendor Unknown
SFPVendorID 0
SFPPartNumber Unknown
SFPRev 0
type Fibre Channel
OperState disabled
PortID 010600
WWN 200600c0ad00cc30
LinkSpeed auto
LinkState Inactive
SyncState SyncLost
LoginStatus NotLoggedIn
Loopback Status Not Running
MaxCredit 12
DonatedToPort None
RunningType Unknown
PendingType gl-port
InBandMgmt enabled
SFPTType NotInstalled
SFPVendor Unknown
SFPVendorID 0
SFPPartNumber Unknown
SFPRev 0
type Fibre Channel
OperState disabled
PortID 010700
WWN 200700c0bd00ac30
LinkSpeed 2Gb/s
LinkState Inactive
SyncState SyncLost
LoginStatus NotLoggedIn
Loopback Status Not Running
MaxCredit 12
DonatedToPort None
RunningType Unknown
PendingType gl-port
InBandMgmt enabled

```

fc6 down

fc7 down

show interface

fc8	down			SFPTType NotInstalled SFPVendor Unknown SFPVendorID 0 SFPPartNumber Unknown SFPRev 0 type Fibre Channel OperState disabled PortID 010800 WWN 200800c0dd00bc30 LinkSpeed auto LinkState Inactive SyncState SyncLost LoginStatus NotLoggedIn Loopback Status Not Running MaxCredit 12 DonatedToPort None RunningType Unknown PendingType gl-port InBandMgmt enabled SFPTType NotInstalled SFPVendor Unknown SFPVendorID 0 SFPPartNumber Unknown SFPRev 0
fc15	up			type Fibre Channel OperState enabled PortID 020f00 WWN 200f00065338bc21 LinkSpeed 2Gb/s LinkState Active SyncState SyncAcquired LoginStatus LoggedIn Loopback Status Not Running MaxCredit 12 DonatedToPort None RunningType f-port PendingType f-port InBandMgmt enabled SFPTType NotApplicable SFPVendor N/A SFPVendorID N/A SFPPartNumber N/A SFPRev N/A
fc11	up			type Fibre Channel loop LOOP READY connection F Port port id 0x20000 datarate 2 Gb/s ALPA 0
fc12	up			firmware READY type Fibre Channel loop LOOP READY connection F Port port id 0x20f00 datarate 2 Gb/s ALPA 0
ge1	up	10.1.10.45/ffffff00	02023da80a51	firmware READY type Gigabit Ethernet mtu 1500 speed 1000000000 flags UP BRDCST RUNNING MLTCST signal signal detect duplex full auto-negotiate complete


```

                                flow control rx pause
                                SFPVendor IBM
                                SFPVendorID 53P1476006FSR
                                SFPPartNumber IBM42P21SNY
                                SFPRev AA102P21SNY
ge2          up    10.3.10.25/ffffff00    02045aa80a51 type Gigabit Ethernet
                                mtu 1500
                                speed 10000000000
                                flags UP BRDCST RUNNING MLTCS
                                signal signal detect
                                duplex full
                                auto-negotiate complete
                                flow control rx pause
                                SFPVendor IBM
                                SFPVendorID 53P1476000XY1
                                SFPPartNumber IBM42P21SNY
                                SFPRev AA102P21SNY

Configuration Data

Interface IP/Netmask                Autonegotiation  Speed Duplex
-----
mgmt      10.1.10.244/ffffff00      enabled          100    full
ha        10.1.20.56/ffffff00       enabled          100    full

Interface Status  Al-    Ext-  Fan-  Link  Loopback  Mfs-    Time  RSCN-  Port-  Port-
                  fairness credit enable speed type  bundle out  enable type  mode
-----
fc1      enabled disabled 0      enabled auto  Unknown  enabled 10    enabled fl-port
fc2      enabled disabled 0      enabled auto  Unknown  enabled 10    enabled gl-port
fc3      enabled disabled 0      enabled auto  Unknown  enabled 10    enabled gl-port
fc4      enabled disabled 0      enabled auto  Unknown  enabled 10    enabled gl-port
fc5      enabled disabled 0      enabled auto  Unknown  enabled 10    enabled gl-port
fc6      enabled disabled 0      enabled auto  Unknown  enabled 10    enabled gl-port
fc7      enabled disabled 0      enabled auto  Unknown  enabled 10    enabled gl-port
fc8      enabled disabled 0      enabled auto  Unknown  enabled 10    enabled gl-port

Interface MTU Size  AutoNegotiation  Vlan    IP/Netmask                Secondary
-----
ge1      1500      autodetect      enabled  10.1.10.45/ffffff00
ge2      1500      autodetect      enabled

```

Table 12-32 describes the fields shown in the display.

Table 12-32 Description of Fields in the “show interface” Command Output

Field	Description
Operational Data	Operational characteristics.
Interface	The interface name.
Stat	The status of the interface.
IP/Netmask	The IP address and subnet mask of the interface.
MAC	The MAC address of the interface.
Options	Configuration and operational information for the interface, including interface type, MTU size, speed, Small Form-factor Pluggable (SFP) module, running and pending port type, and activity information.
Configuration Data	Configuration information. Not all fields are applicable to all interfaces.

Table 12-32 Description of Fields in the “show interface” Command Output (continued)

Field	Description
Interface	The interface name.
IP/Netmask	The IP address and subnet mask of the interface.
AutoNegotiation	For management, HA and Gigabit Ethernet interfaces, the status of autonegotiation (enabled or disabled).
Speed	The port speed.
Duplex	The duplex setting.
Status	For FC interfaces, the status of the interface (enabled or disabled).
AI-fairness	For FC interfaces, the status of the fairness algorithm (enabled or disabled).
Ext-credit	For FC interfaces, the number of extended buffer-to-buffer credits available.
Fan-enable	For FC interfaces, the status of Fabric Address Notification (enabled or disabled).
Link speed	For FC interfaces, the operational transfer rate.
Loopback type	For FC interfaces, the type of loopback test enabled for the interface.
Mfs-bundle	For FC interfaces, the status of Multi-Frame Sequence bundling (enabled or disabled).
Timeout	For FC interfaces, the MFS-bundle timeout value.
RSCN-enable	For FC interfaces, the status of the generation of Registered State Control Notification (RSCN) messages (enabled or disabled).
Port-type	For FC interfaces, the pending port type.
Port-mode	For FC interfaces, the port mode (associated with translated loop port types).
MTU Size	For Gigabit Ethernet interfaces, the size of the maximum transfer unit, in bytes.
Vlan	For Gigabit Ethernet interfaces, the status of VLAN support (enabled or disabled).
Secondary	For Gigabit Ethernet interfaces, the interface assigned as the secondary for the specified IP address.

The following is example output from the **show interface brief** command, using the match expression *type* to limit the options displayed:

```
[SN5428-2A]# show interface brief type
Interface Stat IP/Netmask          MAC          Options
-----
lo0          up    127.0.0.1/ff000000      000000000000 type Loopback
mgmt         up    10.1.10.244/ffffff00    00012d071160 type Ethernet
ha           down
fe12        up    2.0.0.1/ffffff00       00048aa58711 type Ethernet
fc0          up
fc1          up
fc2          down
fc3          down
fc4          down
fc5          down
fc6          down
fc7          down
fc8          down
fc15        up
```



```

fc11      up                                     type Fibre Channel
fc12      up                                     type Fibre Channel
ge1       up   10.1.10.45/ffffff00   02012d020304 type Gigabit Ethernet
ge2       up   10.3.10.23/ffffff00   02034d030405 type Gigabit Ethernet

```

The following is example output from the **show interface stats** command, for the FC interface *fc4*:

```
[SN5428-2A]# show interface fc4 stats
```

Port Attribute	Value	Port Attribute	Value
-----	-----	-----	-----
BytePerf	0	FramePerf	0
TxBytePerf	0	TxFramePerf	0
RxBytePerf	0	RxFramePerf	0
ErrorRates	16		
Login Count	0x6	Logout Count	0x5
Total Errors	0xb	Invalid Dest Addr	0x0
Class2 Frames In	0x0	Class2 Frames Out	0x0
Class3 Frames In	0x93	Class3 Frames Out	0x68
Total Rx Frames	0x93	Total Tx Frames	0x68
Class2 Words In	0x0	Class2 Words Out	0x0
Class3 Words In	0x0	Class3 Words Out	0x87
Total Rx Words	0x0	Total Tx Words	0x87
Decode Error Count	0xb	Loss of Sync Count	0x1
Invalid CRC Count	0x0	Tx Wait Count	0x34
Class3 Toss Count	0x0	FReject Count	0x0
FBusy Count	0x0	Link Failures	0x0
Flow Error Count	0x0	LP_TOV Timeout Count	0x0
Primitive Seq Errors	0x0		
Rx Link Resets	0x0	Rx Offline Seq	0x0
Tx Link Resets	0x0	Tx Offline Seq	0xc
Total Link Resets	0x0	Total Offline Seq	0xc
AL Init Count	0x9	AL Init Error Count	0x1
LIP_F7_F7_Count	0x8	LIP_F7_AL_PS Count	0x1
LIP_F8_F7_Count	0x0	LIP_F8_AL_PS Count	0x0
Total LIPS Received	0x9	LIP_AL_PD_AL_PS Count	0x0

Table 12-33 describes the port attributes shown in the display:

Table 12-33 Description of Port Attributes in the “show interface stats” Command Output

Port Attribute	Description
BytePerf	Total number of bytes processed by this port.
TxBytePerf	Total number of bytes transmitted by this port.
RxBytePerf	Total number of bytes received by this port.
ErrorRates	The error rate for this port.
FramePerf	Total number of frames processed by this port.
TxFramePerf	Total number of frames transmitted by this port.
RxFramePerf	Total number of frames received by this port.
Login Count	Incremented when a user logs in.
Total Errors	Total number of errors detected.

Table 12-33 Description of Port Attributes in the “show interface stats” Command Output (continued)

Port Attribute	Description
Logout Count	Incremented when a user logs out.
Invalid Dest Add	Number of invalid destination addresses received.
Class2 Frames In	Number of class 2 frames received by this port.
Class3 Frames In	Number of class 3 frames received by this port.
Total Rx Frames	Total number of frames received by this port.
Class2 Frames Out	Number of class 2 frames sent by this port.
Class3 Frames Out	Number of class 3 frames sent by this port.
Total Tx Frames	Total number of frames issued by this port.
Class2 Words In	Number of class 2 words received by this port.
Class3 Words In	Number of class 3 words received by this port.
Total Rx Words	Total number of words received by this port.
Class2 Words Out	Number of class 2 words sent by this port.
Class3 Words Out	Number of class 3 words sent by this port.
Total Tx Words	Total number of words issued by this port.
Decode Error Count	Number of decoding errors detected.
Invalid CRC Count	Number of invalid CRCs detected.
Class3 Toss Count	Number of class 3 frames tossed.
FBusy Count	The number of times the switch sent a P_BSY because a Class 2 frame could not be delivered within a specified time period; the number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric that is preventing delivery of this frame.
Flow Error Count	Number of flow errors.
Primitive Seq Errors	Primitive sequence errors detected.
Loss of Sync Count	Number of synchronization losses detected by this port. A loss of synchronization (greater than 100 ms) is detected by the receipt of an invalid transmission word.
Tx Wait Count	Time waiting to transmit when blocked with no credit. Measured in FC Word times.
FReject Count	Number of frames from devices that were rejected.
Link Failures	Number of optical link failures detected by this port. A link failure is a loss of synchronization for a period of time greater than the timeout value or by loss of signal while not in the offline state. A loss of signal causes the switch to attempt to re-establish the link. If the link is not re-established by the time specified, a link failure is counted. A link reset is performed after a link failure.
LP_TOV Timeout Count	Number of times the timeout value on the local port has been triggered.
Rx Link Resets	Number of link reset primitives received from an attached device.
Tx Link Resets	Number of link resets issued by this port.

Table 12-33 Description of Port Attributes in the “show interface stats” Command Output (continued)

Port Attribute	Description
Total Link Reset	Total number of link reset primitives.
Rx Offline Seq	Number of offline sequences received. An OLS is issued for link initialization, an NOS state, or to enter the offline state.
Tx Offline Seq	Number of offline sequences issued by this port.
Total Offline Seq	Total number of offline sequences issues by this port.
AL Init Count	Incremented each time the port begins AL initialization.
LIP_F7_F7_Count	A loop initialization primitive frame used to acquire a valid AL_PA.
LIP_F8_F7_Count	A loop initialization primitive frame used to indicate that a loop failure has been detected at the receiver.
Total LIPS Received	Total number of loop initialization primitives received.
AL Init Error Count	Number of times the port entered initialization and the initialization failed.
LIP_F7_AL_PS Count	This LIP is used to reinitialize the loop. An L_port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop.
LIP_F8_AL_PS Count	This LIP denotes a loop failure detected by the L_port identified by AL_PS.
LIP_AL_PD_AL_PS Count	Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets performed.

Related Commands

Command	Description
interface ge?	Configure various operational parameters associated with the Gigabit Ethernet interface.
interface ha ip-address	Specify the HA interface IP address and subnet mask.
interface mgmt ip-address	Specify the management interface IP address and subnet mask.
setup mgmt	Run the wizard to configure the management interface.
setup cluster	Change the configuration of the high availability environment.

show ip

To display information about the SN 5428-2 Storage Router network, including a variety of protocol stack statistics, use the **show ip** command.

show ip {arp | hosts | rip | tcp | udp}

show ip [icmp | route] stats

show ip route [all]

show ip [interface {if-name | all}] [tcp | udp] stats

Syntax Description

arp	Display the ARP table.
hosts	Display all known hosts on the IP network.
rip	Display Routing Information Protocol (RIP) information.
route	Display the system route table.
tcp	Display active TCP connections.
udp	Display system UDP activity.
icmp stats	Display ICMP-related network statistics.
route stats	Display route-related network statistics.
route all	Display the entire system route table, including non-operational route entries.
interface if-name	Display information for the specified interface only.
interface all	Display information for all interfaces.
tcp stats	Display TCP-related network statistics.
udp stats	Display UDP-related network statistics.
stats	Display all IP-related network statistics.

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

- Use the **show ip** command with the **stats** keyword to display operational network statistics related to the specified protocol. The information displayed depends on the type of protocol specified.
- Use the **arp** keyword to display the ARP table.
- Use the **hosts** keyword to display all known IP hosts on the IP network.

- Use the **rip** keyword to display RIP timers and flags.
- Use the **route** keyword to display the routing table. Use the **all** keyword to display all routes, including non-operational routes. *0.0.0.0/32* is the default route.
- Use the **tcp** keyword to display active TCP connections, including the SN 5428-2 web server and other server tasks.
- Use the **udp** keyword to display User Datagram Protocol (UDP) activity on the system.

Examples

The following is example output from the **show ip stats** command:

```
[SN5428-2A]# show ip stats
IP Statistics:
      Packets Received      123477
Packets Delivered to ULP    121436
      Bad Checksum          0
      Packet too Short      0
      Not Enough Data       0
      Bad Header Length     0
      Bad Packet Length     0
      Fragments Received    0
      Fragments Dropped     0
      Fragments Timed Out   0
      Packets Reassembled   0
      Packets Forwarded     0
Destination Unreachables    2035
      Redirected Packets    0
      Unknown Protocol      6
      Packets Sent          12431
      Fragments Sent        0
      Out of Buffers        0
      No Route              0
      Generic Drop          0
```

The following is example output from the **show ip rip** command. RIP has been enabled and is running on the storage router:

```
[SN5428-2A]# show ip rip
Routing Information Protocol (RIP) Information:
      Invalid Timer: 180
      Enabled Flag: true
      Debug Flag: false
      Running Flag: true
```

The following is example output from the **show ip route** command. For static and RIP routes, the two numbers in brackets indicate the administrative distance and hop count values for the route. For example, the RIP route *10.1.10.0/24* has an administrative distance of 120 and a hop count of 1.

```
[SN5428-2A]# show ip route
Codes: C - connected, S - static, R - RIP
S    0.0.0.0/0 [1/0] via 10.2.0.94, mgmt
R    10.1.10.0/24 [120/1] via 10.1.50.10, ge4
C    10.1.50.0/24 is directly connected, ge4
C    10.1.60.0/24 is directly connected, ge1VLAN160
S    10.1.70.0/24 [1/0] via 10.1.50.12, ge4
S    10.1.70.0/24 [1/0] via 10.1.60.12, ge1VLAN160
C    10.1.90.0/24 is directly connected, ge3
C    10.2.0.0/24 is directly connected, mgmt
C    127.0.0.0/8 is directly connected, lo0
```


■ show ip

Related Commands	Command	Description
	ip rip enable	Enable the storage router to learn dynamic routing using the routing information protocol (RIP).
	ip rip timers	Configure various RIP timers.
	ip route	Add a static route to the SN 5428-2 Storage Router routing table.

show logging

To display the logging table routing rules or to display contents of the log file, use the **show logging** command.

show logging *[[all | last nn] [match expression] | size]*

Syntax Descriptions

all	(Optional) Display all log file entries.
last nn	(Optional) Display the last <i>nn</i> lines from the current log file.
match expression	(Optional) Display all entries that match the specified string or regular expression. String matching is case-sensitive. By default, the last 20 log entries are searched.
size	(Optional) Display the number of messages in the log file and the size of the log file, in bytes.

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

- Use the **show logging** command to display the routing rules in the logging table, which is used to route event messages to the appropriate destinations based on the message level and facility.
- Use the **match expression** parameters to display messages in the log file that match the specified string or regular expression. You can search the entire log file for matching messages or restrict the search to the last *nn* number of messages. If the **match** keyword is used without the **all** or **last** keywords, the search is made against the last 20 entries in the log file.

Examples

The following is example output from the **show logging** command:

```
[SN5428-2A]# show logging
Logging is enabled
```

```
Index Level      Priority Facility  Route
1   notice        5         all       all
2   info          6         all       logfile
3   debug         7         HA        rslog
```

```
Syslog host is enabled, ip-address is 10.1.1.144
```


show logging

The following example matches on a regular expression and displays all messages from the UI or IF facility, or all messages at notice or debug level. Only the last 50 log messages are searched for matches.

```
[sn5428-2a]# show logging last 50 match "(%UI|IF)-|- [67]-)"
Oct 10 13:28:45: %UI-5-EWSSL: Starting SSL OpenSSL 0.9.6e 30 Jul 2002 Port 443
Oct 10 13:28:53: %HA-6-HHMTMEC: HA_monitor_task: monitor event change with scsirouter/foo
Oct 10 13:29:09: %UI-5-NSCL: Successful CLI login from [console]
Oct 10 13:29:09: %UI-6-CCEMCS: Executed command "enable" return code is 0
Oct 10 13:29:14: %UI-6-CCEMCS: Executed command "show logging" return code is 0
```

The following is example output from the **show logging match "Successful"** command. Only the last 20 log entries are searched for matches.

```
[SN5428-2A]# show logging match "Successful"
Apr 10 20:48:13: %UI-5-NSCL: Successful CLI login from [10.1.68.196]
Apr 10 22:15:12: %UI-5-NSCL: Successful CLI login from [10.1.42.120]
May 29 21:43:05: %UI-5-NSCL: Successful CLI login from [console]
```

Related Commands

Command	Description
clear logging table	Clear the SN 5428-2 Storage Router logging table of all entries, or to reset the table to factory defaults.
delete logging	Delete a rule from the logging table.
logging #?	Insert a routing rule entry into the logging table.
logging level	Add rule entries to route storage router event, debug and trace messages to various destinations based on facility and notification level.
logging on	Enable or temporarily disable logging of storage router event message.
logging syslog	Identify a remote syslog host to be used to log messages.

show memory

To display information about memory and related resources, use the **show memory** command.

show memory

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator or Monitor.
----------------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to display information about the storage router memory usage. The show memory command is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.
-------------------------	---

Examples	The following is example output from the show memory command:
-----------------	--

```
[SN5428-2A]# show memory
```

```
Memory: 241445888 Available: 46363968
Free Blocks: 569 Max Free Block Size: 39957504
```

```
Buffer Memory:
```

Buffer	Total	Free	Total	Free	
Pool	Blocks	Blocks	Mbufs	Mbufs	Warnings
System	6925	6802	16384	16256	
Data	8997	8997	16800	16800	
GbE	65536	63494	65696	65696	
iSCSI	3000	3000	3240	3240	

Related Commands	Command	Description
	show buffers	Display information about buffer pools.
	show modules	Display addressing information related to the software modules.
	show stack	Display the memory stack on a per-task basis.
	show task	Display information about the tasks running in the storage router.
	show tech-support	Display a variety of diagnostic information for use by Cisco Technical Support professionals.

show modules

To display addressing information about the modules included in the SN 5428-2 Storage Router, use the **show modules** command.

show modules

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use this command to display the memory locations for each module of the storage router software. The **show modules** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

Examples The following is example output from the **show modules** command:

```
[SN5428-2A]# show modules
Modules
```

MODULE NAME	MODULE ID	GROUP #	TEXT START	DATA START	BSS START
sysInit.out	0xd8fee20	2	0xd84cd40	0xd88beb0	0xd88cf50
crashDump.out	0xd744a50	3	0xd73efc0	0xd743560	0xd7435f0
snmp_trapfuncs.out	0xd744690	4	0xd743d20	0xd743de0	0xd743e18
nuEventsCommon.out	0xd73bac8	5	0xd739590	0xd73b150	0xd73b198
nuEvents.out	0xd738cf8	6	0xd730cf0	0xd736dd0	0xd7377c8
ha.out	0xd72eab0	7	0xd6f0de0	0xd702130	0xd702460
confNode.out	0xd729ee0	8	0xd720d70	0xd728730	0xd7287e0
authServer.out	0xd729cb0	9	0xd70d960	0xd71e350	0xd71e570
drv.out	0xd6d0bb0	10	0xd6a1dc0	0xd6b13c0	0xd6b14bc
geBase.out	0xd6cb200	11	0xd6c69a0	0xd6ca350	0xd6ca3a8
i8254x.out	0xd6cafd0	12	0xd663e30	0xd67bba0	0xd67be30
qlogicBase.out	0xd6a1b88	13	0xd69f410	0xd6a1010	0xd6a10b8
qlogic.out	0xd6a1958	14	0xd45caf0	0xd4b7890	0xd54b7c8
qlogicCpp.out	0xd663bf8	15	0xd65b620	0xd662430	0xd6624f0
qlptBase.out	0xd658068	16	0xd656c40	0xd6578f0	0xd657928
qlptCpp.out	0xd656528	17	0xd653bf0	0xd6557d0	0xd655830
qlptDpp.out	0xd652a40	18	0xd5e3680	0xd5fa500	0xd60d600
encap.out	0xd64d110	19	0xd6496b0	0xd64bfe0	0xd64c060
smlApi.out	0xd647fa8	20	0xd639b00	0xd646240	0xd6464b0
vtp.out	0xd639298	21	0xd631f10	0xd637c90	0xd637dd0

show modules

sysDpp.out	0xd62f8d8	22	0xd62ab00	0xd62e2e0	0xd62e3ac
scsiTargetFE.out	0xd62f660	23	0xd569a50	0xd592c90	0xd59aa38
scsiTcpAuth.out	0xd5e3448	24	0xd5dde00	0xd5e2340	0xd5e23c0
slpcommon.out	0xd5dc2f8	25	0xd5d5e50	0xd5db310	0xd5db3d8
libslp.out	0xd5d46e0	26	0xd5ce270	0xd5d3750	0xd5d3798
slpattr.out	0xd5cced0	27	0xd5c6da0	0xd5cc3d0	0xd5cc408
slpd.out	0xd5c5e20	28	0xd6137e0	0xd623d60	0xd6241d8
slptool.out	0xd5c0db0	29	0xd5bef10	0xd5c0610	0xd5c0648
scsiTcpServer.out	0xd5c0b68	30	0xd3bc7d0	0xd3fa560	0xd3fa97c
ttcp.out	0xd45c8b8	31	0xd42cf60	0xd434110	0xd434838
confMgmt.out	0xd459830	32	0xd4564f0	0xd458980	0xd458b10
hwdmon.out	0xd4595a8	33	0xd44d3b0	0xd453c40	0xd45457c
diagMon.out	0xd42cd28	34	0xd5a20b0	0xd5b46d0	0xd5b52cc
diagCppUtils.out	0xd42cae0	35	0xd449610	0xd44d110	0xd44d3a8
diagCppTests.out	0xd426db8	36	0xd421c10	0xd4264e0	0xd426538
diagDppTests.out	0xd421360	37	0xd55a230	0xd569680	0xd569838
sn5428TestTable.out	0xd4210a8	38	0xd42c230	0xd42c6f0	0xd42ca5c
confXML.out	0xd420e70	39	0xd403560	0xd41e8f0	0xd41e9c8
confObj.out	0xd420c40	40	0xcfc55a50	0xcfafad70	0xcfb04b4
openssl.out	0xd044590	41	0xcce9a10	0xcdd21d0	0xcddc158
sshmgr.out	0xcfc55818	42	0xcfc523f0	0xcfc546c0	0xcfc546e0
clusterApp.out	0xcfc515f8	43	0xcfc46330	0xcfc4f7b0	0xcfc4f81c
cdp.out	0xcfc428e8	44	0xcfc36130	0xcfc40380	0xcfc40958
slpApp.out	0xcfc426a0	45	0xcfc41240	0xcfc41ec0	0xcfc41efc
systemApp.out	0xcfc33bc8	46	0xce7a5a0v0	0xceb5630	0xceb5b34
ipRouter.out	0xcfc24eb0	47	0xcfc1d0a0	0xcfc23270	0xcfc2330c
srMon.out	0xcfc193e8	48	0xcfc10a20	0xcfc17b50	0xcfc17c00
scsiRouter.out	0xcfc19030	49	0xcdd6a0	0xcfc07530	0xcfc07854
frameRacer.out	0xcfc18ba0	50	0xccec70a0	0xccec0c10	0xccec0cdc
authServerApp.out	0xcfc0c8f0	51	0xccebec10	0xccec7010	0xccec708c
fcSwApp.out	0xcfc0c008	52	0xcce14c70	0xcce32170	0xcce337dc
fdisk.out	0xcce67f80	53	0xcce61a80	0xcce66c90	0xcce670bc
sysMon.out	0xcce5fae8	54	0xcce5d6a0	0xcce5f000	0xcce5f0a4
ui.out	0xcce5f688	55	0xc618c20	0xc881aa0	0xc8bcbff4
snmp_util.out	0xcce97d8	56	0xcce82a0	0xcce8f10	0xcce8f68
mib2.out	0xcce7848	57	0xcceb7070	0xccec0d60	0xccec3078
ifx.out	0xcce1cc0	58	0xcdd210v0	0xcce04b0	0xcce0bc8
ether.out	0xcddbfe8	59	0xcdda4d0	0xcddb370	0xcddb6f8
mau_if.out	0xcdd9bf0	60	0xcdd76a0	0xcdd8bd0	0xcdd8fe8
mau_neg.out	0xcdd6930	61	0xcdd50c0	0xcdd5d80	0xcdd6058
entity.out	0xcdd6680	62	0xcceee90	0xcdd0ff0	0xcdd4988
entity_sensor.out	0xccecec50	63	0xccecb20	0xccecd250v0	0xccecddeb8
entity_ext.out	0xccecea08	64	0xcce9c70	0xccecab10	0xccecacf8
entity_fru.out	0xcceb6e38	65	0xcceb46f0	0xcceb5bb0	0xcceb6008
cdp_snmp.out	0xcceb3420	66	0xcceafb40	0xcceb1ec0	0xcceb2378
scsi_mib.out	0xcceaec78	67	0xcce8a440	0xcce92270	0xcce93aa8
fcmgmt_fcsw.out	0xccea86c0	68	0xcce9b660	0xccea32a0	0xccea5d98
syslog_mib.out	0xcce8a208	69	0xcce854c0	0xcce88800	0xcce88d10
config_copy.out	0xcce83b18	70	0xcce7da20	0xcce820d0	0xcce82600
srMonApp.out	0xcce83898	71	0xcce7ce50	0xcce7d9d0v0	0xcce7da0c
snmpApp.out	0xcce83638	72	0xcce88f40v0	0xcce8a040	0xcce8a15c

Related Commands	Command	Description
	show buffers	Display information about buffer pools.
	show memory	Display information about memory and related resources.
	show stack	Display the memory stack on a per-task basis.
	show task	Display information about the tasks running in the storage router.
	show tech-support	Display a variety of diagnostic information for use by Cisco Technical Support professionals.

show restrict

To display current restrictions on the use of the SN 5428-2 Storage Router console, interfaces, and ports, use the **show restrict** command.

show restrict

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use this command to identify the current interface access restrictions.

Examples The following is example output from the **show restrict** command. The output shows that passwords are not enabled for the console. All interfaces are closed to FTP and SSL. The HA and Gigabit Ethernet interfaces are also closed to SSH and Telnet. The Gigabit Ethernet interfaces are closed to HTTP. All interfaces are open to SNMP.

```
[SN5428-2A]# show restrict
```

Interface	Port	Status	Protocol
mgmt	21	closed	ftp
	22	open	ssh
	23	open	telnet
	80	open	http
	161	open	snmp
	443	closed	ssl
ha	21	closed	ftp
	22	closed	ssh
	23	closed	telnet
	80	open	http
	161	open	snmp
	443	closed	ssl
ge1	21	closed	ftp
	22	closed	ssh
	23	closed	telnet
	80	closed	http
	161	open	snmp
	443	closed	ssl


```
ge2      21      closed  tp
         22      closed  ssh
         23      closed  telnet
         80      closed  http
        161      open    snmp
        443      closed  ssl
```

```
Console Passwords: disabled
```

Related Commands

Command	Description
restrict	Secure access to storage router interfaces by communications protocols and services.
restrict console	Enable or disable password checking on the console interface.

show route

To display all static routes that have been configured, including those that have not been added to the routing table because the associated interface is not yet configured, use the **show route** command.

show route

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use this command to display all static routes that have been configured for the storage router, including routes that have been configured but have not been added to the routing table. Use the **show ip route** command to display the entire routing table.



Note A route will not become operational until the associated interface is configured.

Examples The following is example output from the **show route** command. The administrative distance displays after the route information. In this example, there are two static routes. One static route is configured as a default route, and both static routes have the default administrative distance of 1.

```
[SN5428-2A]# show route
ip route default 10.1.10.201 1
ip route 172.16.211.0/24 10.1.10.201 1
```

Related Commands	Command	Description
	ip default-gateway	Configure a gateway for the default route.
	ip route	Add a static route to the SN 5428-2 Storage Router routing table.
	show ip	Display entries from the SN 5428-2 Storage Router routing table and statistics about the protocols used in the storage router network.

show runningconfig

To display the current running configuration of the SN 5428-2 Storage Router, or save the commands used to create the running configuration to a file, use the **show runningconfig** command.

show runningconfig [*to filename*]

Syntax Description

to filename	(Optional) Save the running configuration of the storage router as a series of CLI commands and descriptive text in the specified file. The file will be saved in the <i>script</i> directory.
--------------------	--

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use the **show runningconfig** command to display the current system configuration information as it would be saved to a configuration file. Use the **to** keyword to save the running configuration as a series of CLI commands and descriptive text in the specified file. This file is saved in the *script* directory and can be used as a basis to create command scripts to automate common tasks. Use the **read script** command to execute a command script.



Note

A saved configuration file requires editing before it can be used as a command script via the **read script** command.

[Table 12-34](#) describes the significant elements that are displayed.

Table 12-34 Elements Displayed for the show runningconfig Command

Element	Description
AAA	Authentication, authorization, and accounting method configuration information.
ACCESSLIST	Access list description and entry information.
ADMIN	The storage router administrator contact information.
ADMIN LOGIN	The Administrator mode password.
CDP	Cisco Discovery Protocol configuration, including timer and holdtime settings.
CLUSTER	The name of the cluster to which this storage router belongs.
DNS	The name of any defined domain name servers.

Table 12-34 Elements Displayed for the show runningconfig Command (continued)

Element	Description
FCIP	FCIP instance configuration information.
FC PORTS	Operational characteristics of the Fibre Channel interfaces.
FC SWITCH	Global Fibre Channel attributes.
FC ZONE	Zone configuration information.
FC ZONE ALIAS	Zone alias configuration information.
FC ZONE SET	Zone set configuration information.
GE	IP addresses and operational characteristics of the Gigabit Ethernet interfaces.
HA	HA configuration information.
HA Port	IP address and operational characteristics of the HA interface.
LOGGING ROUTE FACILITY	The logging table.
Mgmt Port	IP address and operational characteristics of the management interface.
MONITOR LOGIN	The Monitor mode password.
RESTRICT	Storage router interface restrictions.
RIP	Routing Information Protocol (RIP) configuration information.
SCSIROUTER	Configuration information for each SCSI routing instance, including name, description, server interface and other instance-specific configuration information.
SNMP	The SNMP settings.
SNTP	Date and time information, including the address of any associated NTP server.
SOFTWARE	The default download location for storage router software.
SSH	Secure Shell (SSH) configuration information.
SYSLOG	Remote logging configuration information.
SYSTEM	SN 5428-2 Storage Router name.
TELNET	Session timeout information.
VLAN	VLAN configuration information.
VTP DOMAIN	VTP domain name.
VTP MODE	VTP configuration mode.

Examples

The following is an example of output from the **show runningconfig** command, for a storage router deployed for SCSI routing:

```
[SN5428-2A]# show runningconfig
!
! CLUSTER
!
! cluster Lab1
!
! ACCESSLIST
```



```

!
accesslist aegis
accesslist aegis 10.2.0.23/255.255.255.255
accesslist aegis 10.3.0.36/255.255.255.255
accesslist aegis 10.4.0.49/255.255.255.255
accesslist aegis iscsi-name ign.1987-05.com.cisco.08.80342789af73ebcdef123.xxx
accesslist aegis iscsi-name ign.1987-05.com.cisco.08.7125abc9af73ebcdef123.xxx
accesslist aegis iscsi-name ign.1987-05.com.cisco.08.1234abecf9876bac00034.xxx
accesslist aegis chap-username 12h7b.lab2.webservices
accesslist aegis chap-username dorothy
accesslist aegis chap-username lab2servp
!
! VTP DOMAIN
!
vtp domain none
!
! VTP MODE
!
vtp mode client
!
! VLAN
!
! (no vlan(s) found)
!
! SCSIROUTER
!
scsirouter zeus
scsirouter zeus authenticate "none"
scsirouter zeus primary "none"
scsirouter zeus reserve proxy disable
scsirouter zeus failover primary none
scsirouter zeus failover secondary none
scsirouter zeus lun reset no
scsirouter zeus serverIf gel 10.1.0.45/255.255.255.0
scsirouter zeus target webserver2 wwpn "21:00:00:05:ae:03:6d:6e"
scsirouter zeus target webserver2 enabled
scsirouter zeus target webserver2 accesslist "aegis"
!
! SYSTEM
!
hostname SN5428-2A
!
! Mgmt Port
!
interface mgmt ip-address 10.1.10.244/255.255.255.0
!
! HA Port
!
interface ha ip-address 10.1.20.56/255.255.255.0
! GE
!
interface ge2 autonegotiation autodetect
interface ge2 mtusize 1500
interface ge2 vlan enable
!
! GE
!
interface gel autonegotiation autodetect
interface gel mtusize 1500
interface gel vlan enable
!
! ROUTES
!
ip route 10.1.30.0/255.255.255.0 10.1.10.201

```


■ show runningconfig

```

ip route 10.1.40.243/255.255.255.255 10.1.10.201
ip route 10.1.50.249/255.255.255.255 10.1.10.201
ip default-gateway 10.1.10.201
!
! RIP
!
no ip rip enable
ip rip timers invalid 180

! ADMIN LOGIN
!
admin password <password>
!
! MONITOR LOGIN
!
monitor password <password>
!
! SNMP
!
clock timezone CST6CDT
ntp peer 10.1.60.86
!
! SNMP
!
snmp-server community public ro
snmp-server community private rw
no snmp-server host all traps
no snmp-server sendauthtraps
snmp-server linkupdown mgmt
snmp-server linkupdown ge1
snmp-server linkupdown ge2
snmp-server linkupdown fc1
snmp-server linkupdown fc2
snmp-server linkupdown fc3
snmp-server linkupdown fc4
snmp-server linkupdown fc5
snmp-server linkupdown fc6
snmp-server linkupdown fc7
snmp-server linkupdown fc8
!
! DNS
!
ip name-server 10.1.40.243 10.1.50.249
ip domain-name mystoragenet.com
!
! TELNET
!
no session-timeout
!
! SSH
!
ssh enable
!
! SOFTWARE
!
software http url "http://www.cisco.com"
software http username "ciscocustomer" password "<password>"
software proxy username none
!
! HA
!
! ha configuration clustered
!
!
```



```
! SYSLOG
!
logging syslog 10.4.5.6
!
! LOGGING ROUTE FACILITY
!
logging level info from all to console logfile
logging level debug from HA to logfile
!
! RESTRICT
!
restrict mgmt ftp
no restrict mgmt telnet
no restrict mgmt http
no restrict mgmt snmp
restrict mgmt rlogin
restrict mgmt ssl
no restrict mgmt ssh
!
restrict ha ftp
restrict ha telnet
no restrict ha http
no restrict ha snmp
restrict ha rlogin
restrict ha ssl
no restrict ha ssh
!
restrict ge1 ftp
restrict ge1 telnet
restrict ge1 http
restrict ge1 snmp
restrict ge1 rlogin
restrict ge1 ssl
no restrict ge1 ssh
!
restrict ge2 ftp
restrict ge2 telnet
restrict ge2 http
restrict ge2 snmp
restrict ge2 rlogin
restrict ge2 ssl
no restrict ge2 ssh
!
!
! CDP
!
cdp enable
cdp timer 60
cdp holdtime 180
cdp interface mgmt enable
cdp interface ha enable
cdp interface ge1 enable
cdp interface ge2 enable
!
! FC SWITCH
!
fcswitch ratov 10000
fcswitch edtov 2000
fcswitch dstov 5000
fcswitch fstov 1000
fcswitch zoning default all
fcswitch zoning autosave enable
fcswitch zoning merge SW2
fcswitch domainid 99 force
```



```

no fcswitch domainid lock enable
fcswitch interop-credit 12
!
! FC ZONE ALIAS
!
fcalias iscsi
fcalias iscsi member wwpn 280000059ac58710
fcalias iscsi member wwpn 290000059ac58710
fcalias foo
fcalias foo member wwpn 20:1b:00:38:15:74:b1:19
!
! FC ZONE
!
zone footest
zone footest member wwpn 201a0381474b118
zone footest member fcalias foo
!
! FC ZONE SET
!
zoneset thor
zoneset thor zone agamemnon
no zoneset thor enable
!
! FC PORT
!
interface fc1 enable
interface fc1 ms-enable enable
no interface fc1 al-fairness enable
interface fc1 fan-enable enable
interface fc1 ext-credit 0
interface fc1 mfs-bundle enable timeout 10
interface fc1 linkspeed auto
interface fc1 type gl-port
!
interface fc2 enable
interface fc2 ms-enable enable
no interface fc2 al-fairness enable
interface fc2 fan-enable enable
interface fc2 ext-credit 0
interface fc2 mfs-bundle enable timeout 10
interface fc2 linkspeed auto
interface fc2 type gl-port
!
interface fc3 enable
interface fc3 ms-enable enable
no interface fc3 al-fairness enable
interface fc3 fan-enable enable
interface fc3 ext-credit 0
interface fc3 mfs-bundle enable timeout 10
interface fc3 linkspeed auto
interface fc3 type gl-port
!
interface fc4 enable
interface fc4 ms-enable enable
no interface fc4 al-fairness enable
interface fc4 fan-enable enable
interface fc4 ext-credit 0
interface fc4 mfs-bundle enable timeout 10
interface fc4 linkspeed auto
interface fc4 type gl-port
!
interface fc5 enable
interface fc5 ms-enable enable
no interface fc5 al-fairness enable

```



```
interface fc5 fan-enable enable
interface fc5 ext-credit 0
interface fc5 mfs-bundle enable timeout 10
interface fc5 linkspeed auto
interface fc5 type gl-port
!
interface fc6 enable
interface fc6 ms-enable enable
no interface fc6 al-fairness enable
interface fc6 fan-enable enable
interface fc6 ext-credit 0
interface fc6 mfs-bundle enable timeout 10
interface fc6 linkspeed auto
interface fc6 type gl-port
!
interface fc7 enable
interface fc7 ms-enable enable
no interface fc7 al-fairness enable
interface fc7 fan-enable enable
interface fc7 ext-credit 0
interface fc7 mfs-bundle enable timeout 10
interface fc7 linkspeed auto
interface fc7 type gl-port
!
interface fc8 enable
interface fc8 ms-enable enable
no interface fc8 al-fairness enable
interface fc8 fan-enable enable
interface fc8 ext-credit 0
interface fc8 mfs-bundle enable timeout 10
interface fc8 linkspeed auto
interface fc8 type gl-port

! AAA
!
aaa new-model
aaa authentication iscsi temp local group radius local-case
username "fred" password "9 af4f2428498a41a31e237de1c4a9b9fcef"
username "pat" password "9 7ddbccc3d0daf013f4293c3d3bd94539dd"
username "kris" password "9 0607167520058771e66ab1d379d7e6505f"
username "adrian" password "9 0ad24a3b35dc296d894e512416d572b3ee"
radius-server retransmit 12
radius-server host 10.5.0.53 auth-port 1645
tacacs-server timeout 12
tacacs-server host 10.7.0.22 auth-port 49
```

The following example creates a command file called *SN5428-2A_script2* in the *script* directory. It contains many of the CLI commands that were issued to create the current running configuration.

```
[SN5428-2A]# show runningconfig to SN5428-2A_script2
```


Related Commands	Command	Description
	read script	Read and execute the CLI commands in the named script file.
	restore all	Restore the contents of the named configuration file into memory.
	save all	Save all configuration information
	show bootconfig	Display the bootable configuration, or create a command file based on the bootable configuration.
	show savedconfig	List the contents of the savedconfig directory or the contents of the named configuration file.
	show script	Display the contents of the script directory or the contents of the named command file.

show savedconfig

To list the available files in the *savedconfig* directory or to view the contents of a specific configuration file, use the **show savedconfig** command. Configuration files are stored in the *savedconfig* directory.

show savedconfig [*filename*]

Syntax Description	<i>filename</i>	(Optional) The name of the configuration file to display. This file must exist in the <i>savedconfig</i> directory and be in the appropriate format.
--------------------	-----------------	--

Defaults	None.
----------	-------

Command Modes	Administrator or Monitor.
---------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to display a list of configuration files in the <i>savedconfig</i> directory before attempting a restore. Use the <i>filename</i> parameter to view the contents of the specified configuration file. You can also use the show scsirouter from or show accesslist from commands to display specific objects from the named configuration file, allowing you to verify that the object of your restore command exists in the selected file.
------------------	---

Examples	The following is example output from the show savedconfig command:
----------	---

```
[SN5428-2A]# show savedconfig
Config_Nov122001
Config_Jul172001
Special_Config
AccessList_Config
```

The following is example output from the **show savedconfig** command using the *filename* parameter:

```
[SN5428-2A]# show savedconfig AccessList_Config
!
! CLUSTER
!
cluster Lab1
!
! ACCESSLIST
!
accesslist aegis
accesslist aegis 10.2.0.23/255.255.255.255
accesslist aegis 10.3.0.36/255.255.255.255
accesslist aegis 10.4.0.49/255.255.255.255
```


Related Commands	Command	Description
	copy	Copy the named configuration or script file from a remote location to the storage router or from the storage router to a remote location.
	delete savedconfig	Remove a saved configuration file from the storage router.
	restore aaa	Restore AAA authentication services from the named configuration file.
	restore accesslist	Restore the named access list or all access lists from the named configuration file.
	restore all	Restore the contents of the named configuration file into memory.
	restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
	restore system	Restore selected system information from the named configuration file.
	restore vlan	Restore VLAN configuration information from the named configuration file.
	save aaa	Save the current AAA configuration information.
	save accesslist	Save configuration data for the named access list or all access lists.
	save all	Save all configuration information.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	save system	Save selected system configuration information.
	save vlan	Save configuration information for the named VLAN or all VLANs.
	show bootconfig	Display the bootable configuration, or create a command file based on the bootable configuration.
	show runningconfig	Display the running configuration, or create a command file based on the running configuration.

show script

To list the available files in the *script* directory or to view the contents of a specific command file, use the **show script** command. Configuration files are stored in the *script* directory.

show script [*filename*]

Syntax Description	<i>filename</i> (Optional) The name of the command file to display. This file must exist in the <i>script</i> directory.
--------------------	--

Defaults	None.
----------	-------

Command Modes	Administrator or Monitor.
---------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to display a list of files in the <i>script</i> directory before attempting to execute the commands in the script using the read script command. Use the <i>filename</i> parameter to view the contents of the specified command file.
------------------	--

Examples	The following is example output from the show script command:
----------	--

```
[SN5428-2A]# show script
MyScriptFile
Lab1_Script
Test_12Nov
MyBoot
```

Related Commands	Command	Description
	copy	Copy the named configuration or script file from a remote location to the storage router or from the storage router to a remote location.
	read script	Read and execute the CLI commands in the named script file.

show scsirouter

To display configuration information and operational statistics related to the named SCSI routing instance or all instances, use the **show scsirouter** command.

show scsirouter

show scsirouter *name* **all**

show scsirouter {*name* | **all**} [**from** {*filename* | **bootconfig** | **runningconfig**}]

show scsirouter {*name* | **all**} **brief**

show scsirouter {*name* | **all**} **connection** [**stats** | **tcp**]

show scsirouter {*name* | **all**} **failover**

show scsirouter **all** **failover** **brief**

show scsirouter {*name* | **all**} **host** [**stats** | **table**]

show scsirouter {*name* | **all**} **serverif** [**from** {*filename* | **bootconfig** | **runningconfig**}]

show scsirouter {*name* | **all**} **stats**

show scsirouter {*name* | **all**} **target** {*name* | **all**} [**from** {*filename* | **bootconfig** | **runningconfig**} | **stats**]

show scsirouter {*name* | **all**} **target** **table**

Syntax Description

<i>name</i>	The name of the SCSI routing instance or the name of the target.
<i>name</i> all	Display all configuration information for the specified SCSI routing instance.
all	Display the requested information for all SCSI routing instances or all targets.
from <i>filename</i>	(Optional) The name of the saved configuration file containing the specified SCSI routing instance information. This file must exist in the <i>savedconfig</i> directory.
from bootconfig	(Optional) Display the requested configuration information from the persistent saved configuration. Use this keyword string to display complete configuration information for a SCSI routing instance from any node in a cluster, even if the instance is not active on that node.
from runningconfig	(Optional) Display the requested configuration information from the currently running configuration.
brief	(Optional) Display status and brief configuration information.
connection	(Optional) Display connection information for the named SCSI routing instance.
failover	(Optional) Display the HA failover information for the named SCSI routing instance.

host	(Optional) Display status and other operational data for IP hosts currently connected to the named SCSI routing instance.
host table	(Optional) Display information about all IP hosts that have attempted to connect to the named SCSI routing instance.
serverif	(Optional) Display configuration information for the Gigabit Ethernet interface associated with the named SCSI routing instance.
stats	(Optional) Display accumulated operational information for the SCSI routing instance. This display shows statistics accumulated since the named SCSI routing instance became active or statistics were last cleared, whichever is more recent.
target	(Optional) Display configuration information related to targets (including the iSCSI Name) associated with the named SCSI routing instance.
target table	Display all targets, target status, and access list associations for the specified SCSI routing instance or all instances, in table format.
tcp	(Optional) Display current and maximum TCP window size for each connected IP host.

Defaults

The **show scsirouter** command with no parameters displays the name of each SCSI routing instance running on this storage router. Unless a specific **from** parameter is specified, any information displayed is from the currently running configuration.

Command Modes

Administrator or Monitor

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

In a cluster environment, a SCSI routing instance can only be active on one storage router at a time. Issue the appropriate **show** commands from the node that is running the instance to display complete configuration information and operational statistics. If you issue **show** commands from a storage router that is not running the instance, operational statistics are not available and configuration information is truncated.



Timesaver

To display complete configuration information for a SCSI routing instance from any storage router in a cluster, even if that SCSI routing instance is not active on that node, use the command **show scsirouter name from bootconfig**.

Use the optional **target** or **serverif** keyword to restrict the display to configuration information related to the specified element. For example:

- The command **show scsirouter name target** displays current configuration information, including access list and iSCSI Name, for all targets associated with the named SCSI routing instance.
- The command **show scsirouter all serverif** displays current configuration information for the Gigabit Ethernet interfaces associated with all SCSI routing instances.

Use the **connection** or **host** keyword to display specific operational data for the named SCSI routing instance.

- The command **show scsirouter name host stats** displays IP host status and operational statistics for currently connected IP hosts for the named SCSI routing instance.
- The command **show scsirouter name host table** displays iSCSI Name, alias, IP address and CHAP user name (if any) for all IP hosts that have attempted to access the named SCSI routing instance. If you are going to use iSCSI Name entries for access control, you can use this command to obtain or verify the iSCSI Name of your IP hosts.
- The command **show scsirouter name stats** displays accumulated operational information about all IP hosts that have been connected since the named instance became active. Operational statistics include logins, active connections, target access and authentication failure information.
- The command **show scsirouter all connection stats** displays connection statistics for all SCSI routing instances.
- The **show scsirouter all stats** command is useful for determining quick operational status of all instances running in the storage router.
- Use the **show scsirouter all** command to display configuration information for all SCSI routing instances, including descriptions, targets and associated access lists.

Examples

The following is example output from the **show scsirouter** command:

```
[SN5428-2A]# show scsirouter
foo
zeus
```

The following is example output from the **show scsirouter stats** command:

```
[SN5428-2A]# show scsirouter all stats
```

Router	Started	Logins Accepted	Logins Active	Target Access Failures	Authentication Failures
zeus	Jul 25 12:40:03	6	5	0	0

1 scsirouter listed

[Table 12-35](#) describes the significant fields in the display.

Table 12-35 Description of Fields in the “show scsirouter stats” Command Output

Field	Description
Router	The name of the SCSI routing instance.
Started	The date and time the SCSI routing instance was last started.
Logins Accepted	The total number of logins accepted since the last time the SCSI routing instance was started or counters were cleared.
Logins Active	The total number of active connections.
Target Access Failures	The total number of times the SCSI routing instance failed to access a target since the last time the SCSI routing instance was started or counters were cleared.
Authentication Failures	If authentication is enabled, the total number of attempts to access storage that failed authentication checks.

The following is example output from the **show scsirouter all host table** command. If you are going to use iSCSI Name entries for access control, you can configure your IP hosts and attempt to access the desired SCSI routing instance. Then issue this command to display the iSCSI Name information, which can be used to populate the desired access list.

```
[SN5428-2A]# show scsirouter all host table
Name:   iqn.1987-05.com.cisco.01.27a2410eae4affa82a81143d70ce10
Alias:  lab1
IP:     10.2.0.23
CHAP username:  742Nlab1
```

The following is example output from the **show scsirouter all failover** command. This command displays both configured and current operational failover information for all the SCSI routing instances in the cluster. [Table 12-36](#) describes the significant fields in this display.

```
[SN4528-2A]# show scsirouter all failover

Each [ ] below contains node operating characteristics for a scsirouter.
[Instance Status, Failover Priority, Eligibility]
Instance Status('M' = Master, ' ' = Slave)
Failover Priority(' ' = none, 'fp' = primary, 'fs' = secondary)
Eligibility(U = Eligibility has not been initialized
             N = None of the configured devices are available or
               a configured interface is unavailable
             S = Some of the configured devices are available
             A = All of the configured devices are available
             P = Primary and all of the configured devices are available)

Scsirouter  Configured Primary  Configured Failover Primary  Configured Failover Secondary  This Node  Failover Node List
-----
R1          none             none             none             [ A]      [MfpA] SN5428-2B
R2          SN5428-2A        none             none             [M P]     [ A] SN5428-2B
R3          SN5428-2A        none             none             [M P]     [ S] SN5428-2B
R4          SN5428-2A        none             none             [M P]     [ N] SN5428-2B
```

Table 12-36 Description of Fields in the “show scsirouter all failover” Command Output

Field	Description
Scsirouter	The name of the SCSI routing instance in the cluster.
Configured Primary	The name of the storage router configured as the primary for the SCSI routing instance, if any.
Configured Failover Primary	If a failover list has been explicitly configured for the SCSI routing instance, the first storage router in the list.
Configured Failover Secondary	If a failover list has been explicitly configured for the SCSI routing instance, the second storage router in the list.
This Node	The instance status, failover priority and eligibility information for the storage router from which the command was issued.
Failover Node List	The instance status, failover priority and eligibility information for the indicated node, in the order that the nodes appear in the failover list.

The following is example output from the **show scsirouter all failover brief** command. This command shows the eligibility of each SCSI routing instance for each storage router in the cluster.

```
[SN5428-2A]# show scsirouter all failover brief
Descriptions of eligibility ranked from most eligible to least:
  Primary = This node is configured as primary and
            all of the configured devices are available
  All = All of the configured devices are available to this node
  Some = Some of the configured devices are available to this node
  None = None of the configured devices are available to this node
        or a configured interface is unavailable
  Unknown = Eligibility information has not been initialized

Scsirouter SN5428-2A  SN5428-2B
-----
R1          All       All
R2          Primary   All
R3          Primary   Some
R4          Primary   None
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
clear counters scsirouter	Reset accumulated operational statistics for the specified SCSI routing instance.
delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
save scsirouter	Save configuration information for the named SCSI routing instance.
save system	Save selected system configuration information.
scsirouter enable	Stop or start the named SCSI routing instance.
scsirouter failover	Add the storage router to the HA failover list for the specified SCSI routing instance.
scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
scsirouter target maxcmdqueuedepth	Specify the maximum number of commands allowed at any given time from each iSCSI session to the specified target.
setup scsi	Run the wizard to configure a SCSI routing instance.

show sessions

To display information about active Telnet, SSH or GUI sessions to the SN 5428-2 Storage Router, use the **show sessions** command.

show sessions {all | cli | gui}

Syntax Description	all	Display all active Telnet or GUI management sessions.
	cli	Display only active CLI sessions.
	gui	Display only active GUI sessions.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.
	3.3.1	The maximum number of concurrent sessions was changed to 16.

Usage Guidelines There are a maximum of 16 concurrent management sessions per storage router. The sessions are restricted as follows:

- One session is reserved for the EIA/TIA-232 console interface.
- There can be a maximum of seven CLI sessions via Telnet or SSH.
- There can be a maximum of eight GUI sessions via HTTP or HTTPS.

Examples The following is example output from the **show sessions** command. The asterisk designates the CLI management session from which the command was issued.

```
[SN5428-2A] # show sessions all
```

```

      Id Auth      From          Login
-----
*  1  monitor  console      Mar 22 17:19:10 [TELNET]
   2  admin   10.1.40.212  Mar 22 11:44:46 [TELNET]
   3  admin   10.3.12.222  Mar 22 11:47:12 [GUI]
```

```
3 of 16 sessions
```


Related Commands	Command	Description
	admin password	Set the login password for administrative access to the storage router management interface.
	monitor password	Set the login password for view-only access to the storage router management interface.
	session-timeout	Set the number of minutes a management session to the storage router can be inactive before the session times out.

show slp

To display the status of the Service Location Protocol (SLP) service and the interface address where the SLP service is listening for incoming SLP service requests, use the **show slp** command.

show slp

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to display the operational status of the SLP service. The SLP listens on all configured IP interfaces.

Examples

The following is example output from the **show slp** command:

```
[SN5428-4A]# show slp

SLP is RUNNING

Listening interfaces:
  127.0.0.1          TCP LISTEN
  10.1.40.116       TCP LISTEN      UDP MULTICAST  UDP UNICAST
  10.1.20.116       TCP LISTEN      UDP MULTICAST  UDP UNICAST
```

Related Commands

Command	Description
scsirouter slp enable	Enable the advertisement of the targets of the named SCSI routing instance with the SLP service.
slp findattrs	Discover the attributes of a specific SLP registered service.
slp findsrvs	Locate a SLP registered service of a specific type on the local subnet.
slp findsrvtypes	Discover all SLP registered service types on the local subnet.

show snmp

To display SNMP management configuration information for the SN 5428-2 Storage Router, use the **show snmp** command.

show snmp

Syntax Description This command has no arguments or keywords.


Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use the **show snmp** command to review the SNMP configuration settings before changing those settings with the **snmp-server** command.

The command displays IP addresses of the destination hosts used for notifications (traps), the name of the SNMP community having read access to the storage router network (get-community), and the name of the community having write access to the storage router network (set-community), the version of traps to be sent, and configuration information for Send Authentication, Entity Field Replaceable Unit (FRU), and Link Up/Down traps.

 **Note** The community names are only displayed when the command is issued from an Administrator mode session.

Examples The following is example output from the **show snmp** command, issued from an Administrator mode session:

```
[SN5428-2A]# show snmp
First Trap Host: 10.1.30.17, will be sent version 1 traps
Second Trap Host: <none found or defined>
Get Community String: public
Set Community String: mynetmanagers
Send Authentication Traps: enabled
Send Entity FRU Traps: enabled
Link Up/Down Enable for mgmt: enabled
Link Up/Down Enable for ha: disabled
Link Up/Down Enable for fc1: enabled
Link Up/Down Enable for fc2: enabled
Link Up/Down Enable for fc3: disabled
Link Up/Down Enable for fc4: enabled
Link Up/Down Enable for fc5: disabled
Link Up/Down Enable for fc6: enabled
```



```
Link Up/Down Enable for fc7: enabled
Link Up/Down Enable for fc8: disabled
Link Up/Down Enable for ge1: enabled
Link Up/Down Enable for ge2: enabled
System location is: Test lab
```

Related Commands

Command	Description
setup netmgmt	Run the wizard to configure network management.
snmp-server	Configure the storage router for SNMP management.

show software version

To display a list of software versions available on the SN 5428-2 Storage Router, use the **show software version** command.

show software version {v.x.y | all | boot | current}

Syntax Description		
all		Display information about all versions of software available on the storage router.
v.x.y		Display information about the specified software version, including the download file name.
boot		Display information about the version of software that will run when the system is rebooted, including the download file name.
current		Display information about the version of software that is currently running on the storage router, including the download file name.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use the **show software version all** command to display the size of each version of software and the date and time it was built. The display also shows the version of software currently running and the version which will be booted when the system is reset. It includes the protocol and default location from which new software is available for download and the amount of disk space currently available for new software.

Examples The following is example output from the **show software version all** command:

```
[SN5428-2A]# show software version all
Version          Boot  Hash  Sign  Crash      Size  Date
-----
3.3.1-K9         OK    OK    N/A    0    11229.0 KB  Jan 10 09:57 CDT 2003

      Http Url: http://www.cisco.com
      Http Username: phurley
      Http Password: *****

      Proxy Address:
      Proxy Port:
      Proxy Url:
      Proxy Username:
      Proxy Password:
```



```

Tftp Hostname:
Tftp Directory:

Software Space Available: 34250.0 KB
Current Version: 3.3.1-K9
Boot Version: 3.3.1-K9

```

The following example displays the download file name for the currently running version of software:

```

[SN5428-2A]# show software version current

Version          Boot  Hash  Sign  Crash      Size  Date
-----
3.3.1-K9         OK   OK   N/A   0    11229.0 KB  Dec 10 09:57 CDT 2002

Download File Name
-----
sn5428-2-sw-3.3.1-K9.tar

      Http Url: http://www.cisco.com
      Http Username: phurley
      Http Password: *****

      Proxy Address:
      Proxy Port:
      Proxy Url:
      Proxy Username:
      Proxy Password:

      Tftp Hostname:
      Tftp Directory:

Software Space Available: 34250.0 KB
Current Version: 3.3.1-K9
Boot Version: 3.3.1-K9

```

Related Commands

Command	Description
delete software version	Remove the specified version of software from the storage router.
download software	Download the list of available software versions or the specified version of software from the named location.
save all	Save all configuration information.
save system	Save selected system configuration information.
software version	Specify the version of software to run when the storage router is restarted.
verify software version	Check the specified software version for problems.

show ssh

To display Secure Shell (SSH) server configuration, use the **show ssh** command.

show ssh

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator and Monitor.
----------------------	----------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to verify SSH is configured for the storage router and that the SSH service is running. If the SSH server is enabled and the SSH service is running, you can still restrict SSH access for specific interfaces by using the restrict command.
-------------------------	---

Examples	The following is example output from the show ssh command:
-----------------	---

```
[SN5428-2A]# show ssh

SSH Server Configuration

          Status: enabled
```

Related Commands	Command	Description
	restrict	Secure access to storage router interfaces by communications protocols and services.
	show restrict	Display configurable security settings for the storage router interfaces.
	show sessions	Display information about active Telnet, SSH or GUI sessions to the storage router.
	show ssh fingerprint	Display SSH key generation status and current public key information.
	ssh enable	Enable SSH and start the SSH service.
	ssh keygen	Generate the SSH public and private key pairs for the storage router.

show ssh fingerprint

To display the status of SSH key generation and the current public key information for the SN 5428-2 Storage Router, use the **show ssh fingerprint** command.

show ssh fingerprint

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator and Monitor.
----------------------	----------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	<p>Use this command to display the status of the SSH key generation process and to display the existing public key information, including the number of bits used to generate the keys.</p> <p>Before generating new SSH keys, use this command to verify the key generation process is not currently in process.</p>
-------------------------	---


Examples	The following is example output from the show ssh fingerprint command:
-----------------	---

```
[SN5428-2A]# show ssh fingerprint
Key generation status is 'Idle'

1024 da:35:91:9a:fe:70:20:a7:b0:2f:d2:0e:b1:6c:6f:10 admin@SN5428-2A

1024 7f:5e:95:9c:3b:cc:10:eb:62:76:a4:88:48:08:2c:de /ata3/ssh/ssh_host_rsa_key.pub

1024 10:a6:aa:52:6a:ac:44:8a:6f:5f:21:2e:6b:1a:da:fa /ata3/ssh/ssh_host_dsa_key.pub
```


 show ssh fingerprint

Related Commands	Command	Description
	restrict	Secure access to storage router interfaces by communications protocols and services.
	show restrict	Display configurable security settings for the storage router interfaces.
	show sessions	Display information about active Telnet, SSH or GUI sessions to the storage router.
	show ssh	Display SSH server configuration.
	ssh enable	Enable SSH and start the SSH service.
	ssh keygen	Generate the SSH public and private key pairs for the storage router.

show stack

To display usage of the stack on a per-task basis, use the **show stack** command.

show stack

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Administrator and Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines The **show stack** command is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.

Examples The following is example output from the **show stack** command:

```
[techpubs2]# show stack
Stack Usage by Task
```

NAME	ENTRY	TID	SIZE	CUR	HIGH	MARGIN
tExcTask	excTask	df fe3b8	7984	240	936	7048
tLogTask	logTask	df fba30	4984	224	288	4696
tCrashDump	crashDumpTas	d73dd08	8176	160	224	7952
utilMonitor	0x000d8600b8	ca7ca98	9984	296	816	9168
tShell	shell	d909598	39056	464	1072	37984
tSysMon	sysMonRun(in	ce5cd48	4088	144	1144	2944
cppNode	IpNodeLocal	d78ac88	9992	232	712	9280
cppListen	IpNodeLocal	d788360	9984	384	584	9400
dpp0Node	IpNodeLocal	d7859a8	9984	232	712	9272
qlFc1	QlogicFC::sc	cc73de8	9992	208	2344	7648
qlFc2	QlogicFC::sc	cb18de8	9992	208	2344	7648
tAuthServ	authServerTa	ca6aca0	15984	448	880	15104
tFtpdTask	0x00000ea660	d930698	11984	336	464	11520
HA_main	HA_main_task	c96da38	9992	376	2480	7512
tNuLogWatche	tNuLogWatche	cce75b8	16368	600	1592	14776
entropyd	0x000cf5397c	c986878	16368	144	864	15504
sshmgr	0x000cf53704	c982188	16376	312	376	16000
ewTelnetd	0x000c6882a8	c97df70	8176	240	304	7872
VTP	Vtp::task(vo	ca73630	9992	256	1392	8600
tSnmpd	0x0000050af0	ca9e808	28664	1920	2472	26192
tProtoCDP	cdp_prot(voi	ca77848	16368	272	3192	13176
tCfgCopy	listWatcher(ccae9e8	16368	200	328	16040
HA_newcfg	HA_newcfg_ta	c979c00	15984	200	3832	12152

■ show stack

```

HA_monitor      HA_monitor_t  c975b68  15984  208  1984  14000
HA_appctrl      HA_appctrl_t  c971ad0  15984  240  5760  10224
hdwMonitor      0x000d452410 cab9de8   9984  144  1328   8656
sensorMntr      entitySensor  ca861a8   9984  152   280   9704
eeScratch       ExeEng::scra  d781c40  19984  184  1336  18648
cppEeIpc        ExeEng::ipcT  d772db0  39984  488  3824  36160
dpp0EeIpc       ExeEng::ipcT  d75f100  39984  488  3760  36224
nuLogTask       LogTask::tas  ccc9a58  19984  200 10456   9528
tSnmpTmr        0x00000508d0 caa0f78   4080  248   312   3768
tSMLMgr         0x000d642c8c ca82f78   9992 3736  4560   5432
tfeTask         ScsiTargetGl  c8e39c0   9992  160   712   9280
cppEeJob        ExeEng::jobT  d77cc08  39984  168  1848  38136
dpp0EeJob       ExeEng::jobT  d768f58  39984  168   648  39336
tNetTask        netTask       da0c958  19984  208  1352  18632
ui              tEmWeb        ca53b60  49144 4376 22944 26200
tSntpcMon       SntpConf::sn  cc700c8   7984  224  1904   6080
slpTask         slpd_task     ca63b30  32760  448  1448  31312
srMonitor       srMonitor(vo  ca55d78   8176  384  5064   3112
tFcSwMon        FcSwApp::fcs  c97bd58   7984  352  4272   3712
idleTask        0x000d8603a4 ca7a170   9984  136   568   9416
INTERRUPT              5000    0   928   4072

```

Table 12-37 describes the fields in the display.

Table 12-37 Description of Fields in the “show stack” Command Output

Field	Description
NAME	The name of the task.
ENTRY	The task entry point.
TID	The task ID.
SIZE	The maximum size of the task, in bytes.
CUR	The current size of the task.
HIGH	The largest size of the task since the storage router was last started.
MARGIN	The margin between the size of the task and the size in the HIGH field.

Related Commands

Command	Description
show buffers	Display information about buffer pools.
show memory	Display information about memory and related resources.
show modules	Display addressing information related to the software modules.
show task	Display information about the tasks running in the storage router.
show tech-support	Display a variety of diagnostic information for use by Cisco Technical Support professionals.

show static

To display the currently configured IP host to Fibre Channel (FC) address mappings saved in the storage router, use the **show static** command. This command is only available when the storage router is deployed for static transparent SCSI routing.

show static iscsibindings

Syntax Description	iscsibindings	Display the IP host to FC mappings that are currently configured in the storage router.
--------------------	---------------	---

Defaults	None.
----------	-------

Command Modes	Administrator and Monitor.
---------------	----------------------------

Command History	Release	Modification
	3.3.1	This command was introduced.

Usage Guidelines	When the storage router is deployed for static transparent SCSI routing, the IP host to FC address mappings are saved and retained in the storage router when it is restarted. Use the show static iscsibindings command to display the mappings that are currently configured in the storage router.
------------------	--

Examples

The following example displays the currently configured mappings:

```
[SN5428-2A]# show static iscsibindings
```

Interface	WWPN	Host IP Address	Host Name
fci1	280100065338d6c0	10.1.20.2	iscsi.cisco.testlab
fci1	280200065338d6c0	10.1.4.213	iqn.1987-05.com.cisco.02.0AB08...B6E5CCE.WIN1
fci2	290100065338d6c0	10.1.30.100	iqn.1987-05.com.cisco.02.9FD389...36D3D3.NT10

Related Commands	Command	Description
	clear static	Clear the mapping of the IP host to Fibre Channel (FC) address for the specified WWPN.

show system

To display a variety of system information about the SN 5428-2 Storage Router, including system name and deployment option, use the **show system** command. A table of information about storage router network interfaces also displays.

```
show system [from {filename | bootconfig | runningconfig}]
```

Syntax Description	from filename	(Optional) Display the system configuration information from the specified configuration file. This file must exist in the <i>savedconfig</i> directory.
	from bootconfig	(Optional) Display the system configuration information from the persistent saved configuration, used when the storage router is restarted.
	from runningconfig	(Optional) Display the system configuration information from the currently running configuration.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Use the **show system** command to quickly display information about the system configuration, including system name, current software version, date and time, NTP server, name server and domain information.

Use the **from** keyword to display system configuration from the specified configuration file, the system bootable configuration, or the currently running configuration. The system information is displayed in the same format as the **show bootconfig** output.

Examples

The following is example output from the **show system** command:

```
[SN5428-2A]# show system
      System Name: SN5428-2A
      System Deployed For: SCSI routing
      Software Capacity: 59392.0 KB
      Free Software Space: 34350.0 KB
      Configuration Capacity: 14464.0 KB
      Free Configuration Space: 14174.0 KB
      Log Capacity: 29056.0 KB
      Free Log Space: 28892.0 KB
      Software Version: 3.3.1-K9
      Last Reset: Wed Dec 18 20:40:53 GMT+6 2002
      Current Time: Wed Dec 18 22:30:57 GMT+6 2002
      Time Zone: Etc/GMT+6
      NTP Server: 10.1.60.86
      Name Servers: 10.1.40.243 (Pri) 10.1.50.249 (Sec)
```



```

Domain: mystoragenet.com
Telnet session timeout: 15

```

```

          Model Number  Rev  Serial Number  Part Number
System      SN 5428-2-K9  A0   SAD051301XB   800-21476-01
Processor   RME060702     A0   SAD05130130   73-7996-04

Device      IP/Netmask                      MAC
lo0         127.0.0.1/8                    00:00:00:00:00:00
mgmt        10.1.10.244/24                 00:01:2c:06:13:70
ha          10.1.20.56/24                 00:01:64:40:ef:c1
ge1
ge2         10.1.0.45/24                   02:02:3d:01:1c:a5

```

Table 12-38 describes the fields in the display.

Table 12-38 Description of Fields in the “show system” Command Output

Field	Description
System Name	The name of the storage router.
System Deployed For	The deployment option (SCSI routing or Transparent SCSI routing).
Software Capacity	The amount of space allocated for software, in kilobytes.
Free Software Space	Total software capacity currently available, in kilobytes.
Configuration Capacity	The amount of space allocated for configuration files, in kilobytes.
Free Configuration Space	Total configuration capacity currently available, in kilobytes.
Log Capacity	The amount of space allocated for log files, in kilobytes.
Free Log Space	Total log capacity currently available, in kilobytes.
Software Version	The version of software that is currently running, such as 3.3.1-K9.
Last Reset	The date and time the system was last reset.
Current Time	The current date and time.
Time Zone	The time zone in which this storage router is located.
NTP Server	The IP address of the time server.
Name Servers	The IP address of the primary and secondary DNS servers.
Domain	The domain to which the storage router belongs.
Telnet session timeout	The amount of time a management session can be inactive before it is timed out, in minutes.
Model Number	The model number for the SN 5428-2 system and processor.
Rev	The revision number for the SN 5428-2 system and processor.
Serial Number	The serial number for the SN 5428-2 system and processor.
Part Number	The part number for the SN 5428-2 system and processor.
Device	The name of the interface.
IP/Netmask	The IP address and subnet mask associated with the named interface.
MAC	The machine address associated with the named interface.

The following is example output from the **show system from bootconfig** command:

```

!
! SYSTEM
!
hostname SN5428-2A
!
! Mgmt Port
!
interface mgmt ip-address 10.1.10.244/255.255.255.0
!
! HA Port
!
interface ha ip-address 10.1.20.56/255.255.255.0
!
! GE
!
interface ge1 autonegotiation autodetect
interface ge1 mtusize 1500
interface ge1 vlan enable
!
! GE
!
interface ge2 autonegotiation autodetect
interface ge2 mtusize 1500
interface ge2 vlan enable
!
! ROUTES
!
ip default-gateway 10.1.10.201
ip route 10.1.30.0/255.255.255.0 10.1.10.201
!
! RIP
!
no ip rip enable
ip rip timers invalid 180
!
! ADMIN LOGIN
!
admin password <password>
!
! MONITOR LOGIN
!
monitor password <password>
!
! SNMP
!
ntp peer 10.1.60.86
clock timezone Etc/GMT+6
!
! SNMP
!
snmp-server community public ro
snmp-server community private rw
no snmp-server host all traps
no snmp-server sendauthtraps
snmp-server linkupdown mgmt
snmp-server linkupdown ha
snmp-server linkupdown fei2
snmp-server linkupdown fci1
snmp-server linkupdown fci2
snmp-server linkupdown ge1
snmp-server linkupdown ge2
snmp-server linkupdown fc0

```



```
snmp-server linkupdown fc1
snmp-server linkupdown fc15
snmp-server linkupdown fc2
snmp-server linkupdown fc3
snmp-server linkupdown fc4
snmp-server linkupdown fc5
snmp-server linkupdown fc6
snmp-server linkupdown fc7
snmp-server linkupdown fc8
!
! DNS
!
ip name-server 10.1.40.243 10.1.50.249
ip domain-name cisco.com
!
! TELNET
!
session-timeout 15
!
! SSH
!
ssh enable
!
! SOFTWARE
!
software http url "http://www.cisco.com"
software http username phurley
software proxy username <password>
!
! HA
!
! ha configuration clustered
!
! LOGGING ROUTE FACILITY
!
logging level notice from all to all
logging level info from all to logfile
!
! RESTRICT
!
restrict mgmt ftp
no restrict mgmt telnet
no restrict mgmt http
no restrict mgmt snmp
restrict mgmt ssl
no restrict mgmt ssh
!
restrict ha ftp
no restrict ha telnet
no restrict ha http
restrict ha snmp
restrict ha ssl
restrict ha ssh
!
restrict gel ftp
no restrict gel telnet
restrict gel http
restrict gel snmp
restrict gel ssl
restrict gel ssh
```


show system

```

!
restrict ge2 ftp
no restrict ge2 telnet
restrict ge2 http
restrict ge2 snmp
restrict ge2 ssl
restrict ge2 ssh
!
!
! CDP
!
cdp enable
cdp timer 60
cdp interface mgmt enable
cdp interface ha enable
cdp interface ge1 enable
cdp interface ge2 enable

```

Related Commands

Commands	Description
hostname	Specify the storage router system name.
ip name-server	Specify the IP addresses of a primary (and optional secondary) DNS.
logging syslog	Identify a remote syslog host to be used to log messages.
ntp peer	Specify the name or IP address of the NTP server with which the storage router will synchronize date and time.
save all	Save all configuration information.
software version	Specify the version of software to run when the storage router is restarted.
verify software version	Check the specified software version for problems.

show task

To display information about tasks running in the SN 5428-2 Storage Router, issue the **show task** command.

show task {*task-id* | **all**}

Syntax Description	<i>task-id</i>	The TID for a specific task, obtained from the show task all display. Prefix the TID with <i>0x</i> , which indicates a hex number.
	all	Display information about all running tasks.

Defaults None.

Command Modes Administrator and Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use the **show task** command to view priority, status, and error information for all tasks, and register and stack trace information for a specific task. To display The **show task** command is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.

Examples The following is example output from the **show task all** command:

```
[SN5428-2A]# show task all
Running Tasks
```

NAME	ENTRY	TID	PRI	STATUS	PC	SP	ERRNO	ELAY
tExcTask	excTask	df fe3b8	0	PEND	10eaf8	df fe2c8	3006b	0
tLogTask	logTask	df fba30	0	PEND	10eaf8	df fb950	0	0
tCrashDump	crashDumpTas	d73dd08	0	PEND	b68b8	d73dc68	0	0
utilMonitord8600b8		ca7ca98	1	DELAY	bb2c4	ca7c970	0	42
tShell	shell	d909598	1	PEND	10eaf8	d9093c8	c0002	0
tSysMon	sysMonRun__F	ce5cd48	2	DELAY	bb2c4	ce5ccb8	0	2229
cppNode	nodeTaskExec	d78ac88	40	PEND	b68b8	d78aba0	0	0
cppListen	listener__12	d788360	40	PEND	b68b8	d7881e0	0	0
dpp0Node	nodeTaskExec	d7859a8	40	PEND	b68b8	d7858c0	0	0
qlFc1	scsiTask__8Q	cc73de8	45	PEND+T	b68b8	cc73d18	3d0004	101
qlFc2	scsiTask__8Q	cb18de8	45	PEND+T	b68b8	cb18d18	3d0004	101
tAuthServ	authServerTa	ca6aca0	50	PEND	b68b8	ca6aae0	0	0
tFtpdTask	ea660	d930698	55	PEND	b68b8	d930548	0	0
HA_main	HA_main_task	c96da38	77	PEND	b68b8	c96d8c0	380003	0
tNuLogWatchtNuLogWatche		cce75b8	78	PEND	10eaf8	cce7360	c0002	0
entropyd	cf5397c	c986878	78	DELAY	bb2c4	c9867e8	0	25
sshmgr	cf53704	c982188	78	PEND	b68b8	c982050	0	0
ewTelnetd	c6882a8	c97df70	78	PEND	b68b8	c97de80	0	0

■ show task

```

ui          tEmWeb          ca53b60  79  READY          bbd34  ca53480      0      0
VTP         task__3Vtp      ca73630  80  PEND           10eaf8  ca73530      0      0
tSnmpd      50af0          ca9e808 150  PEND           b68b8   ca9e088      0      0
tProtoCDP   cdp_prot__Fv             ca77848 150  PEND           10eaf8  ca77738      0      0
tCfgCopy    listWatcher_         ccae9e8 160  PEND           b6fd8   ccae920      0      0
HA_newcfg   HA_newcfg_ta            c979c00 160  DELAY          bb2c4   c979b38    380003    111
HA_monitor  HA_monitor_t           c975b68 160  DELAY          bb2c4   c975a98    3d0002     81
HA_appctrl  HA_appctrl_t           c971ad0 160  PEND           10eaf8  c9719e0    380003      0
hdwMonitor  d452410                cab9de8 180  DELAY          bb2c4   cab9d58      0    11318
sensorMntr  entitySensor           ca861a8 180  PEND           b68b8   ca86110      0      0
eeScratch   scratchTask_           d781c40 200  PEND           b68b8   d781b88      0      0
cppEeIpc    ipcTaskExec_           d772db0 200  PEND           b68b8   d772bc8      46      0
dpp0EeIpc   ipcTaskExec_           d75f100 200  PEND           b68b8   d75ef18      46      0
nuLogTask   task__7LogTa           ccc9a58 200  PEND           b68b8   ccc9990    c0002      0
tSnmpTmr    508d0                  caa0f78 200  PEND           10eaf8  caa0e80      0      0
tSMLMgr     d642c8c                ca82f78 200  PEND+T          b68b8   ca820e0    3d0004    138
tfeTask     tfeTask__19S           c8e39c0 200  DELAY          bb2c4   c8e3920      0      50
cppEeJob    jobTaskExec_           d77cc08 201  READY          b68b8   d77cb60      31      0
dpp0EeJob   jobTaskExec_           d768f58 201  READY          b68b8   d768eb0      0      0
tNetTask    netTask                 da0c958 202  READY          b68b8   da0c888      0      0
tSntpcMon   sntpcMon_tas           cc700c8 248  DELAY          bb2c4   cc6ffe8    710005   312264
slpTask     slpd_task              ca63b30 248  PEND           b68b8   ca63970    380003      0
srMonitor   srMonitor__F           ca55d78 248  DELAY          bb2c4   ca55bf8      0     139
tFcSwMon    fcswMon_Task           c97bd58 248  DELAY          bb2c4   c97bbf8      0     541
idleTask    d8603a4                ca7a170 249  READY          b72dc   ca7a0e0      0      0

```

The following is example output from the **show task** command for TID “dffb30”. Because the TID is a hex number, the TID must be prefixed with *0x*.

```
[SN5428-2A]# # show task 0xdffb30
Registers
```

NAME	ENTRY	TID	PRI	STATUS	PC	SP	ERRNO	DELAY
tLogTask	logTask	dffb30	0	PEND	10eaf8	dffb950	0	0

```
stack: base 0xdffb30 end 0xdffa6a8 size 4984 high 288 margin 4696
```

```
options: 0x6
```

```
VX_UNBREAKABLE      VX_DEALLOC_STACK
```

```

r0   =      0   sp   = dffb950  r2   =      0   r3   =      0
r4   =      0   r5   =      0   r6   =      0   r7   =      0
r8   =      0   r9   =      0  r10   =      0  r11   =      0
r12  =      0  r13   =      0  r14   =      0  r15   =      0
r16  =      0  r17   =      0  r18   =      0  r19   =      0
r20  = 180000  r21   = 170000  r22   = 170000  r23   = 180000
r24  = 180000  r25   = 180000  r26   = 180000  r27   = ffffffff
r28  = 10000003 r29   = 10000010 r30   = dffbc4c  r31   =      0
msr  =    b030  lr   =      0  ctr   =      0  pc   = 10eaf8
cr   = 42000000 xer   =      0

```

```
Stack Trace
```

```

f5218 vxTaskEntry   +60 : logTask ()
9d684 logTask        +30 : msgQReceive ()
b5594 msgQReceive    +298: qJobGet ()

```


Related Commands	Command	Description
	show buffers	Display information about buffer pools.
	show memory	Display information about memory and related resources.
	show modules	Display addressing information related to the software modules.
	show stack	Display the memory stack on a per-task basis.
	show tech-support	Display a variety of diagnostic information for use by Cisco Technical Support professionals.

show tech-support

To display the results of several CLI **show** commands useful for debugging purposes, use the **show tech-support** command.

show tech-support

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines The **show tech-support** command is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.

Use this command to display the output of the following commands, based on the storage router deployment option:

- show system
- show clock
- show software version all
- show cluster
- show admin
- show interface brief
- show interface all
- show interface all stats
- show ip arp
- show ip hosts
- show ip route
- show ip tcp
- show ip udp
- show ip stats
- show ip icmp stats
- show ip route stats
- show ip tcp stats

- `show ip udp stats`
- `show snmp`
- `show devices`
- `show accesslist all`
- `show scsirouter all`
- `show bootconfig`
- `show runningconfig`
- `show ha node stats`
- `show ha app list stats`
- `show ha app all stats`
- `show diagnostics`
- `show boot`
- `show memory`
- `show task all`
- `show stack`
- `show modules`
- `show buffers`
- `show debug scsirouter all tfestatus`
- `show debug fcswitch all`
- `show debug mailboxtrace all`
- `show debug rawlundatabase all`
- `show fcswitch global-nameserver brief`
- `show fcswitch nameserver brief`
- `show debug fcswitch tech-support`

Examples

The following is abbreviated example output from the **show tech-support** command:

```
[SN5428-2A] # show tech-support

*****
*
*   show tech
*
*****
Generated: Fri Mar 22 22:05:20 GMT 2002
System Name: SN5428-2A
*****
*
*   show system
*
*****
```


Related Commands	Command	Description
	show accesslist	Display the contents of the named access list or all access lists.
	show admin	Display system administrator contact information.
	show boot	Display system boot information and startup file parameters.
	show bootconfig	Display the bootable configuration, or create a command file based on the bootable configuration.
	show buffers	Display information about buffer pools.
	show clock	Display the current system date and time, including the system time zone.
	show cluster	Display cluster-related operational statistics, including heartbeat information.
	show debug	Display debug trace information for the specified SCSI routing instance.
	show devices	Display a list of devices discovered on the Fibre Channel interface.
	show diagnostics	Display hardware diagnostic test results.
	show ha	Display HA operational statistics for the storage router or for a specific application.
	show interface	Display operational and configuration information for the specified interface or all interfaces.
	show ip	Display entries from the SN 5428-2 Storage Router routing table, and statistics about the protocols used in the storage router network.
	show memory	Display information about memory and related resources.
	show modules	Display addressing information related to the software modules.
	show runningconfig	Display the running configuration, or create a command file based on the running configuration.
	show scsirouter	Display configuration and operational information for the named SCSI routing instance.
	show snmp	Display the SNMP management configuration information for the storage router.
	show software version	Display a list of software versions available on the storage router, including the currently running version and the version that will run the next time the storage router is restarted.
	show stack	Display the memory stack on a per-task basis.
	show system	Display selected system information, including system name.
	show task	Display information about the tasks running in the storage router.

show telnet

To display the status of the SN 5428-2 Storage Router Telnet server, use the **show telnet** command.

show telnet

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator and Monitor.
----------------------	----------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	Use this command to display the status of the Telnet server. The Telnet server is enabled and running on the storage router by default. If the Telnet server is enabled, you can still restrict Telnet access to the storage router for specific interfaces by using the restrict command.
-------------------------	---

Examples	The following is example output from the show telnet command:
-----------------	---

```
[SN5428-2A]# show telnet

Telnet Server Configuration

      Status: enabled
```

Related Commands	Command	Description
	restrict	Secure access to storage router interfaces by communications protocols and services.
	telnet enable	Enable Telnet and start the Telnet server.

show version

To display version information for system-level software and applications, use the **show version** command.

show version

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use the **show version** command for version information about the storage router operating system software, system bootstrap, application software, and CLI.

Examples The following is example output from the **show version** command:

```
[SN5428-2A]# show version
```

```
CISCO SN 5428-2 Storage Router
```

```

  CLI Version: 2.1
  iSCSI Version: 0/2 (Min/Max)
  System Bootstrap: 3.3.1-K9
  Operating System: 3.3.1-K9
  Application: 3.3.1-K9
  Web Server: R6_1_0
  OpenSSH: 3.4p1
  OpenSSL: 0.9.6e
  Zlib: 1.1.4
```

```
Copyright (c) 1986-2002 by Cisco Systems, Inc
```

Table 12-39 describes the fields in the display.

Table 12-39 Description of Fields in the “show version” Command Output

Field	Description
CLI Version	The command line interface version number.
iSCSI Version	The iSCSI draft version information (minimum and maximum version that can be used with the SCSI routing instance).

Table 12-39 Description of Fields in the “show version” Command Output (continued)

Field	Description
System Bootstrap	The version of software that will run when the storage router is next restarted.
Operating System	The version of software that is currently running.
Application	The current application version.
Web Server	The version number of the SN 5428-2 web server software.
OpenSSH	The version number of the OpenSSH software, for SSH support.
OpenSSL	The version number of OpenSSL software, for SSL support.
Zlib	The version number of the zlib compression library.

Related Commands

Command	Description
show software version	Display a list of software versions available on the storage router, including the currently running version and the version that will run the next time the storage router is restarted.

show vlan

To view configuration and operational information about the specified VLAN, use the **show vlan** command.

```
show vlan [id vid] [brief]

show vlan [id vid] from {filename | bootconfig | runningconfig}
```

Syntax Description

id vid	(Optional) ID of the VLAN to be displayed.
brief	(Optional) Display name, status, and ports for each VLAN.
config	(Optional) Display detailed configuration information for the specified VLAN or all manually configured VLANs.
from filename	Display the configuration information for the specified VLAN or all manually configured VLANs from the specified configuration file. This file must exist in the <i>savedconfig</i> directory.
from bootconfig	Display the configuration information for the specified VLAN or all manually configured VLANs from the persistent saved configuration, used when the storage router is restarted.
from runningconfig	Display the configuration information for the specified VLAN or all manually configured VLANs from the currently running configuration.

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

A VLAN is a group of independent devices that communicate as if they are on the same physical LAN segment but can actually be located anywhere on the network. The storage router dynamically obtains VLAN information from the switch attached to the Gigabit Ethernet interface. Use the **show vlan** command to learn of any VLANs configured on the attached network.



Note

VLANs can be manually configured when the storage router is in VTP Transparent mode.

Examples

The following is example output from the **show vlan** command, followed by example output from the **show vlan config** command for the VLAN ID *101*:

```
[SN5428-2A]# show vlan
```

VLAN	Name	Status	Ports
101	vlanfoo1	active	ge1, ge2
102	vlanfoo2	active	ge2

VLAN	Type	MTU	Interfaces
101	enet	1500	ge2VLAN101
102	enet	1500	ge2VLAN102

```
[SN5428-2A]# show vlan id 101 config
```

```
vlan 101 name vlanfoo1 mtu 1500
```

Related Commands

Command	Description
restore vlan	Restore VLAN configuration information from the named configuration file.
save all	Save all configuration information, including VLAN information.
save scsirouter	Save configuration information for the named SCSI routing instance.
save system	Save selected system configuration information, including VLAN information.
save vlan	Save configuration information for the named VLAN or all VLANs.
scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
show vtp	Display configuration and operational information for VTP.
vlan	Configure a non-VTP VLAN on the storage router.
vtp domain	Assign a VTP domain name to the storage router.
vtp mode	Configure the storage router to operate in client or transparent VTP mode.

show vtp

To display general configuration and status information about the VLAN Trunking Protocol (VTP), use the **show vtp** command.

show vtp [config | stats]

Syntax Description	config	(Optional) Display mode and domain information.
	stats	(Optional) Display operational statistics.

Defaults	None.
----------	-------

Command Modes	Administrator or Monitor.
---------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	VTP must be in transparent mode to configure VLANs. Use the show vtp command to view the current VTP configuration.
------------------	--

Examples	The following is example output from the show vtp command, with the storage router in VTP Client mode:
----------	---

```
[SN5428-2A]# show vtp
Configuration Revision   : 0
Number of existing VLANs : 2
VTP Operating Mode       : Client
VTP Domain Name          : lab1
```

The following is example output from the **show vtp** command, with the storage router in VTP Transparent mode:

```
[SN5428-2A]# show vtp
Configuration Revision   : 0
Number of existing VLANs : 2
VTP Operating Mode       : Transparent
VTP Domain Name          :
```

The following is example output from the **show vtp config** command:

```
[SN5428-2A]# show vtp config
vtp mode client
vtp domain lab1
```


The following is example output from the **show vtp stats** command:

```
[SN5428-2A]# show vtp stats
Summary advertisements received : 3
Subset advertisements received : 2
Request advertisements received : 5
Request advertisements transmitted : 5
```

Related Commands

Command	Description
restore vlan	Restore VLAN configuration information from the named configuration file.
save all	Save all configuration information, including VLAN information.
save scsirouter	Save configuration information for the named SCSI routing instance.
save system	Save selected system configuration information, including VLAN information.
save vlan	Save configuration information for the named VLAN or all VLANs.
scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
show vlan	Display configuration and operational information for the specified VLAN or all VLANs.
vlan	Configure a non-VTP VLAN on the storage router.
vtp domain	Assign a VTP domain name to the storage router.
vtp mode	Configure the storage router to operate in client or transparent VTP mode.

show zone

To display configuration and operational information for Fibre Channel fabric zones from the local zoning database, use the **show zone** command.

show zone {*name* | **all** | **brief**}

Syntax Description

<i>name</i>	Display member type and value for the specified zone.
all	Display member type and value for all zones.
brief	Display member value only for all zones.

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to display member type and value information for all zones known to the local storage router zoning database.

Examples

The following is example output from the **show zone brief** command. The zone named *testlab* has nine members, including an alias named *testgroupA* and 8 devices identified by WWPNs.

```
[SN5428-2A]# show zone brief
Zone Name      Member value
-----
testlab        testgroupA
                201b491585c21911
                201c2301221155b9
                1121334455617681
                2233445566616567
                2233445566616572
                2233445566616573
                1121334455617688
                1121334455617684

1 zone
```


Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	delete fcalias	Delete the named alias or the specified alias member.
	delete zone	Delete the specified Fibre Channel zone or the specified member of the zone from the zoning database.
	delete zoneset	Delete the specified zone from the zone set or to delete the entire named zone set from the zoning database.
	fcalias	Create an alias entity for use in Fibre Channel zoning.
	fcalias member	Add the specified member to the named alias.
	fcswitch zoning autosave	Enable the SN 5428-2 Storage Router to save zoning changes received from switches in the fabric.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	fcswitch zoning merge	Set zoning merge compliance.
	show debug fcswitch	Display internal Fibre Channel interface parameters.
	show fcswitch	Display information about aliases and their members.
	show fcswitch fabric	Display information about the Fibre Channel fabric.
	show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
	zone	Create a Fibre Channel fabric zone.
	zone member	Add a device or an alias to a zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset enable	Activate a zone set.
	zoneset zone	Add a member zone to a zone set.

show zoneset

To display configuration and operational information for Fibre Channel fabric zone sets, use the **show zoneset** command.

```
show zoneset {name | all | brief}
```

Syntax Description	<i>name</i>	Display the member count for the specified zone set.
	all	Display configuration information for all zone sets.
	brief	Display the active flag and the member count only for all zone sets.

Defaults	None
----------	------

Command Modes	Administrator or Monitor.
---------------	---------------------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use this command to display configuration information for zone sets, including the name and number of zones in the zone set and the active flag. This command displays information from the local storage router zoning database.

Examples The following is example output from the **show zoneset brief** command. The zone set named *labservices* is the active zone set and includes nine members.

```
[SN5428-2A]# show zoneset brief
Zoneset Name      Active Member Count
-----
labservices       true      9
```


Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	delete fcalias	Delete the named alias or the specified alias member.
	delete zone	Delete the specified Fibre Channel zone or the specified member of the zone from the zoning database.
	delete zoneset	Delete the specified zone from the zone set or to delete the entire named zone set from the zoning database.
	fcalias	Create an alias entity for use in Fibre Channel zoning.
	fcalias member	Add the specified member to the named alias.
	show debug fcswitch	Display internal Fibre Channel interface parameters.
	show devices	Display a variety of debug information or perform specific troubleshooting activities for Fibre Channel zones.
	show fcswitch	Display information about aliases and their members.
	show fcswitch fabric	Display information about the Fibre Channel fabric.
	show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
	zone	Create a Fibre Channel fabric zone.
	zone member	Add a device or an alias to a zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset enable	Activate a zone set.
	zoneset zone	Add a member zone to a zone set.

slp findattrs

To discover the attributes of a specific Service Location Protocol (SLP) registered service, use the **slp findattrs** command.

slp findattrs *service* [*attribute*]

Syntax Description

<i>service</i>	The SLP service. Use the slp findsrvs command to locate the specific service.
<i>attribute</i>	Display the value of the specified service attribute.

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to verify that the attributes of advertised targets associated with a SCSI routing instance are correct.

Use the **slp findsrvs** command to display the service information used as arguments in the command.

Examples

The following example discovers the attributes of all *iscsi:target* services:

```
[SN5428-2A]# slp findattrs iscsi:target

(iscsi-name=iqn.1987-05.com.cisco.00.dd6b75bc42ef.chimaera_apps), (alias=chimaera_apps),
(portal-group=1), (auth-addr=any), (auth-name=an)
(iscsi-name=iqn.1987-05.com.cisco.00.d621b8e50a31.chimaera_web), (alias=chimaera_web),
(portal-group=1), (auth-a)
```

The following example discovers the value of the *alias* attribute for all *iscsi:target* services:

```
[SN5428-2A]# slp findattrs iscsi:target alias

(alias=chimaera_apps)
(alias=chimaera_web)
```


Related Commands	Command	Description
	scsirouter slp enable	Enable the advertisement of the targets of the named SCSI routing instance with the SLP service.
	show slp	Display the status of the SLP service and the interface address where the SLP service is listening for incoming SLP service requests.
	slp findsrvs	Locate a SLP registered service of a specific type on the local subnet.
	slp findsrvtypes	Discover all SLP registered service types on the local subnet.

slp findsrvs

To locate a Service Location Protocol (SLP) registered service of a specific type on the local subnet where the SN 5428-2 Storage Router is located, use the **slp findsrvs** command.

slp findsrvs *service* [(*attribute=value*)]

Syntax Description	<i>service</i>	The SLP service type. For example, the SLP service type for iSCSI targets is <i>iscsi:target</i> .
	<i>attribute=value</i>	Display the specified service attribute value pair. The attribute value pair must be displayed in parenthesis.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Use this command to verify that a SCSI routing instance that is enabled for SLP is registering its accessible targets with the SLP service. The command displays the URLs for the specified SLP registered service types if they are available on the local subnet.

To display a list of all SLP registered service types found on the local subnet, use the **slp findsrvtypes** command. To display attributes for a specific SLP registered service, use the **slp findattrs** command.

Examples

The following is example output from the **slp findsrvs** command. In this example, two targets are found at address 10.1.10.10. The URL includes the iSCSI Name for each target. The targets belong to a SCSI routing instance with a Gigabit Ethernet interface IP address of 10.1.10.10. The SCSI routing instance may be located on the local storage router or on another SN 5428-2 in the network.

```
[SN5428-2A]# slp findsrvs iscsi:target
```

```
service:iscsi:target://10.1.10.10:3260/ign.1987-05.com.cisco:00.d875b8262ff6.disk1,64432
service:iscsi:target://10.1.10.10:3260/ign.1987-05.com.cisco:00.bd0e6aa3eb51.disk2,64432
```

The following example discovers all SCSI routing instance targets with an alias of *disk1*:

```
[SN5428-2A]# slp findsrvs iscsi:target (alias=disk1)
```

```
service:iscsi:target://10.1.10.10:3260/ign.1987-05.com.cisco:00.d875b8262ff6.disk1,64432
```


Related Commands	Command	Description
	scsirouter slp enable	Enable the advertisement of the targets of the named SCSI routing instance with the SLP service.
	show slp	Display the status of the SLP service and the interface address where the SLP service is listening for incoming SLP service requests.
	slp findattrs	Discover the attributes of a specific SLP registered service.
	slp findsrvtypes	Discover all SLP registered service types on the local subnet.

slp findsrvtypes

To discover all Service Location Protocol (SLP) registered services on the local subnet where the SN 5428-2 Storage Router is located, use the **slp findsrvtypes** command.

slp findsrvtypes

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Administrator or Monitor.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use this command to invoke an SLP user agent tool which looks for SLP registered services on the local subnet. If any SLP services are found, a list of the service types and URLs displays. If SCSI routing instances have SLP enabled and have targets advertised with SLP, the display lists an available SLP service of type *iscsi:target*.

Examples The following is example output from the **slp findsrvtypes** command:

```
[SN5428-2A]# slp findsrvtypes
service:iscsi:target
```

Related Commands	Command	Description
	scsirouter slp enable	Enable the advertisement of the targets of the named SCSI routing instance with the SLP service.
	show slp	Display the status of the SLP service and the interface address where the SLP service is listening for incoming SLP service requests.
	slp findattrs	Discover the attributes of a specific SLP registered service.
	slp findsrvs	Locate a SLP registered service of a specific type on the local subnet.

snmp-server

To configure SNMP management on the SN 5428-2 Storage Router, use the **snmp-server** command. To disable SNMP management or specific host or traps, use the **no** forms of this command.

snmp-server community *community-name* {**ro** | **rw**}

snmp-server host *A.B.C.D* [**version** *version-number*] **traps**

snmp-server linkupdown {**all** | *if-name*}

snmp-server location *text-string*

snmp-server {**sendauthtraps** | **sendfrutraps**}

no snmp-server host {*A.B.C.D* | **all**} **traps**

no snmp-server linkupdown {*if-name* | **all**}

no snmp-server {**sendauthtraps** | **sendfrutraps**}

Syntax Description

<i>community-name</i>	The name of the community having the specified access (read or write) to the storage router. Enclose the string in quotation marks.
ro	Read-only access. The storage router will respond to this community's GET commands. The default SNMP getcommunity is <i>public</i> .
rw	Read/write access. The storage router will respond to this community's SET commands. The default SNMP setcommunity is <i>private</i> .
host <i>A.B.C.D</i>	The IP address of the first destination host used for notifications (traps). <i>A.B.C.D</i> is the dotted quad notation of the IP address. If the command is issued twice, the second IP address becomes the second destination host used for notifications. Version 1 traps will be sent by default.
version <i>version-number</i>	(Optional) The SNMP version for the traps. Use 1 to specify version 1 traps; use 2 to specify version 2 traps.
traps	Keyword, indicating the specified version of traps will be send to the designated host.
host all	Remove all destination hosts used for SNMP notifications (traps).
linkupdown <i>if-name</i>	Enable or disable SNMP link up/down traps for the specified interface. See Table 12-40 for a list of valid interface names.
linkupdown all	Enable or disable SNMP link up/down traps for all interfaces.
location <i>text-string</i>	Provide site-specific location information. If the text string includes spaces or special characters, enclose it in quotation marks. Enter a maximum of 255 characters.
sendauthtraps	Enable or disable authentication failure traps sent when an SNMP request is received with an incorrect community name.
sendfrutraps	Enable or disable entity field replaceable unit (FRU) traps sent when FRU changes occur.

Defaults

The default read-only community name is *public*. This is also known as the *getcommunity*. The default read/write community name is *private*. This is also known as the *setcommunity*. SNMP notifications are disabled by default.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

A variety of network management methods may be used with the storage router, including SNMP. All management methods are enabled by default.

The first issuance of the **snmp-server host** command sets an initial destination host used for traps; the second issuance of the command sets an additional destination host. Version 1 traps are sent by default. To send other trap versions, use the **snmp-server host** command with the **version** keyword.

Link up/down traps can be sent for any valid storage router interface.

Table 12-40 Valid Interface Names

Interface Name	Description
mgmt	The management interface.
ha	The HA interface.
fc?	The Fibre Channel interface, for example, fc1 or fc5.
ge?	The Gigabit Ethernet interface, for example, ge1 or ge2.

Examples

The following command identifies the IP address *10.3.4.200* as a destination host for SNMP Version 1 traps. You can configure two destination hosts for traps.

```
[SN5428-2A] # snmp-server host 10.3.4.200 traps
```

The following command enables the storage router to send authentication failure traps to the SNMP destination host:

```
[SN5428-2A] # snmp-server sendauthtraps
```

The following command enables the storage router to send SNMP link up/down traps for all interfaces to the SNMP destination host:

```
[SN5428-2A] # snmp-server linkupdown all
```

The following command enables the storage router to send SNMP entity FRU insert/remove traps to the SNMP destination host:

```
[SN5428-2A] # snmp-server sendfrutraps
```


Related Commands	Command	Description
	setup mgmt	Run the wizard to configure the management interface.
	setup netmgmt	Run the wizard to configure network management.
	show snmp	Display the SNMP management configuration information for the storage router.

software http url

To configure the default location from which to download updated software to the SN 5428-2 Storage Router via HTTP protocol, use the **software http url** command.

```
software http url {http://servername/path | none}
```

Syntax Description	<i>http://servername/path</i>	The complete URL identifying the location from which to download storage router software.
	none	Delete the current download location and leave the URL blank. Use this keyword to prevent software downloads via HTTP protocol.

Defaults The default download location is <http://www.cisco.com>.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Updated SN 5428-2 software is available from the Cisco.com website. It can also be downloaded and stored locally, then transferred to the storage router when necessary via the **software http url** command. To see the location defined as the current default download location, issue the **show software version all** command.

Examples The following command sets the default download location to the URL <http://www.lab-foo.com/~sn5428-2>:

```
[SN5428-2A] # software http url http://www.lab-foo.com/~sn5428-2
```


Related Commands	Command	Description
	download software	Download the list of available software versions or the specified version of software from the named location.
	save all	Save all configuration information, including default download location for updated SN 5428-2 software.
	save system	Save selected system configuration information, including default download location for updated SN 5428-2 software.
	show software version	Display a list of software versions available on the storage router, including the currently running version and the version that will run the next time the storage router is restarted.
	software http username	Configure the user name and optional password required to access the default download location.
	software proxy	Configure HTTP proxy information.
	software proxy url	Specify the default location from which to download updated SN 5428-2 software via HTTP, using a proxy server.
	software proxy username	Configure the user name and optional password required to access the proxy URL.
	software tftp	Specify the default location from which to download updated SN 5428-2 software via TFTP.
	software version	Specify the version of software to run when the storage router is restarted.
	verify software version	Check the specified software version for problems.

software http username

To configure an optional user name and password used to retrieve updated SN 5428-2 software from the HTTP download location, use the **software http username** command.

```
software http username {webserver-username | none} [password webserver-password]
```

Syntax Description

<i>webserver-username</i>	The user name required to retrieve SN 5428-2 software from the download location.
none	Indicates user name and password are not required. Sets these values to <i>none</i> . This is the default setting.
<i>webserver-password</i>	(Optional) The password required to retrieve SN 5428-2 software from the download location.

Defaults

By default, the user name and password are set to *none*.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use the **show software version all** command to display the current user name configured for retrieval of updated SN 5428-2 software from the HTTP download location.

Use the keyword **none** to indicate that the web server does not require a user name and password to download software, effectively changing the user name and password values to *none*. This is the default setting.

See the **software http url** command for details on setting the location from which to download software.

Examples

The following example sets the user name for HTTP download to *FooAdmin* and the password to *foo*:

```
[SN5428-2A]# software http username FooAdmin password foo
```


Related Commands	Command	Description
	download software	Download the list of available software versions or the specified version of software from the named location.
	save all	Save all configuration information, including default download location for updated SN 5428-2 software.
	save system	Save selected system configuration information, including default download location for updated SN 5428-2 software.
	show software version	Display a list of software versions available on the storage router, including the currently running version and the version that will run the next time the storage router is restarted.
	software http url	Specify the default location from which to download updated SN 5428-2 software via HTTP.
	software proxy	Configure HTTP proxy information.
	software proxy url	Specify the default location from which to download updated SN 5428-2 software via HTTP, using a proxy server.
	software proxy username	Configure the user name and optional password required to access the proxy URL.
	software tftp	Specify the default location from which to download updated SN 5428-2 software via TFTP.
	software version	Specify the version of software to run when the storage router is restarted.
	verify software version	Check the specified software version for problems.

software proxy

To configure the address and port of a proxy server to be used when downloading updated software to the SN 5428-2 Storage Router via HTTP protocol, use the **software proxy** command.

software proxy address *address* [**port** *nn*]

software proxy port *nn*

Syntax Description	<i>address</i>	The IP address or URL of the proxy server. To remove a proxy server address, set the address string to blank, using “ ”.
	<i>nn</i>	(Optional) The port number of the proxy server.

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	The proxy server will be used to access the proxy URL for HTTP download of software for the storage router. To change the port specification without changing the address, use the software proxy port command. Use the software proxy url command to configure the default download location.
------------------	--

Examples	The following example configures the proxy address as <i>10.1.10.126</i> and port as <i>32</i> : [SN5428-2A] # software proxy address 10.1.10.126 port 32
----------	---

Related Commands	Command	Description
	download software	Download the list of available software versions or the specified version of software from the named location.
	save all	Save all configuration information, including default download location for updated SN 5428-2 software.
	save system	Save selected system configuration information, including default download location for updated SN 5428-2 software.
	show software version	Display a list of software versions available on the storage router, including the currently running version and the version that will run the next time the storage router is restarted.
	software http url	Specify the default location from which to download updated SN 5428-2 software via HTTP.
	software http username	Configure the user name and optional password required to access the default download location.
	software proxy url	Specify the default location from which to download updated SN 5428-2 software via HTTP, using a proxy server.
	software proxy username	Configure the user name and optional password required to access the proxy URL.
	software tftp	Specify the default location from which to download updated SN 5428-2 software via TFTP.
	software version	Specify the version of software to run when the storage router is restarted.
	verify software version	Check the specified software version for problems.

software proxy url

To configure the default location from which to download updated software to the SN 5428-2 Storage Router via HTTP protocol using the configured proxy server, use the **software proxy url** command.

software proxy url {*http://servername/path* | **none**}

Syntax Description

<i>http://servername/path</i>	The complete URL identifying the location from which to download SN 5428-2 software via the configured proxy server.
none	Delete the current proxy download location and leave the URL blank. Use this keyword to prevent software downloads via the proxy server.

Defaults

The proxy URL is set to *none*.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

If you use a proxy server to access locations on the Internet, configure the proxy server address and port number using the **software proxy address** command. The proxy server will be used to access the proxy URL when downloading updated SN 5428-2 software.

Examples

The following example configures the proxy address as *10.1.10.126* and port as *32* and then sets the proxy download URL to *http://www.foo-a.com*:

```
[SN5428-2A] # software proxy address 10.1.10.126 port 32
[SN5428-2A] # software proxy url http://www.foo-a.com
```


Related Commands	Command	Description
	download software	Download the list of available software versions or the specified version of software from the named location.
	save all	Save all configuration information, including default download location for updated SN 5428-2 software.
	save system	Save selected system configuration information, including default download location for updated SN 5428-2 software.
	show software version	Display a list of software versions available on the storage router, including the currently running version and the version that will run the next time the storage router is restarted.
	software http url	Specify the default location from which to download updated SN 5428-2 software via HTTP.
	software http username	Configure the user name and optional password required to access the default download location.
	software proxy	Configure HTTP proxy information.
	software proxy username	Configure the user name and optional password required to access the proxy URL.
	software tftp	Specify the default location from which to download updated SN 5428-2 software via TFTP.
	software version	Specify the version of software to run when the storage router is restarted.
	verify software version	Check the specified software version for problems.

software proxy username

To configure a user name and an optional password to be used to retrieve updated SN 5428-2 software from the proxy download location, use the **software proxy username** command.

```
software proxy username {webserver-username | none} [password webserver-password]
```

Syntax Description

<i>webserver-username</i>	The user name required to retrieve SN 5428-2 software from the proxy download location.
none	Indicates user name and password are not required. Sets these values to <i>none</i> . This is the default setting.
<i>webserver-password</i>	(Optional) The password required to retrieve SN 5428-2 software from the proxy download location.

Defaults

By default, the user name and password are set to *none*.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use the **show software version all** command to display the current user name used to retrieve updated SN 5428-2 software from the proxy download location.

Use the keyword **none** to indicate that the web server does not required a user name and password to download software, effectively changing the user name and password values to *none*. This is the default setting.

See the **software proxy url** command for details on setting the location from which to download software.

Examples

The following example sets the user name for proxy download to *FooAdmin* and the password to *foo*:

```
[SN5428-2A]# software proxy username FooAdmin password foo
```


Related Commands	Command	Description
	download software	Download the list of available software versions or the specified version of software from the named location.
	save all	Save all configuration information, including default download location for updated SN 5428-2 software.
	save system	Save selected system configuration information, including default download location for updated SN 5428-2 software.
	show software version	Display a list of software versions available on the storage router, including the currently running version and the version that will run the next time the storage router is restarted.
	software http url	Specify the default location from which to download updated SN 5428-2 software via HTTP.
	software http username	Configure the user name and optional password required to access the default download location.
	software proxy	Configure HTTP proxy information.
	software proxy url	Specify the default location from which to download updated SN 5428-2 software via HTTP, using a proxy server.
	software tftp	Specify the default location from which to download updated SN 5428-2 software via TFTP.
	software version	Specify the version of software to run when the storage router is restarted.
	verify software version	Check the specified software version for problems.

software tftp

To configure host and directory information to be used when downloading updated software to the SN 5428-2 Storage Router via the Trivial File Transfer Protocol (TFTP), use the **software tftp** command.

software tftp directory {*directory_name* | **none**}

software tftp hostname *hostname* [**directory** *directory_name*]

Syntax Description	<i>directory_name</i>	The name of the TFTP base directory.
	none	Remove the directory setting, effectively disabling the use of TFTP protocol.
	<i>hostname</i>	The name of the remote TFTP host. To remove the TFTP configuration, set the host name to blank, using “ ”.

Defaults

None.

Command Modes

Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

Use this command to set the required TFTP parameters for downloading software updates via TFTP protocol. If the base directory is the default, *tftpboot*, omit the directory keyword.

Use the **show software version all** command to display the current TFTP settings.

Examples

The following example sets the TFTP hostname to *TFTPHost1* and the directory to */mytftp*:

```
[SN5428-2A]# software tftp hostname TFTPHost1 directory /mytftp
```


Related Commands	Command	Description
	download software	Download the list of available software versions or the specified version of software from the named location.
	save all	Save all configuration information, including default download location for updated SN 5428-2 software.
	save system	Save selected system configuration information, including default download location for updated SN 5428-2 software.
	show software version	Display a list of software versions available on the storage router, including the currently running version and the version that will run the next time the storage router is restarted.
	software http url	Specify the default location from which to download updated SN 5428-2 software via HTTP.
	software http username	Configure the user name and optional password required to access the default download location.
	software proxy	Configure HTTP proxy information.
	software proxy url	Specify the default location from which to download updated SN 5428-2 software via HTTP, using a proxy server.
	software proxy username	Configure the user name and optional password required to access the proxy URL.
	software version	Specify the version of software to run when the storage router is restarted.
	verify software version	Check the specified software version for problems.

software version

To specify the version of software to run the next time the SN 5428-2 Storage Router is restarted, use the **software version** command. This command forces a system reset and changes the running version of SN 5428-2 software.

software version *v.x.y*

Syntax Description	<i>v.x.y</i>	The version of software to be run when the system is reset.
Defaults	None.	
Command Modes	Administrator.	
Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

This command performs necessary system modifications to assure that the new software version can be run. It causes a system reset, and the new version of software will be run when the reset is complete.

In a cluster environment, this command may temporarily suspend normal HA communications, causing a failover of any SCSI routing instances active on the storage router. Any instances with the **primary** attribute set to name of this SN 5428-2 will resume running on the storage router after it is rebooted.

Use the **show software version all** command to display the list of available versions, the currently running version, and the boot version that will run when the system is reset.

Examples

The following is example output from the **software version** command:

```
[SN5428-2A]# software version 3.3.1-K9
Module                Size    Status    MD5 Digest
-----
vxWorks               3538262 OK        88f817ff917bceb3d1467b593200e1cf
vxWorks.sym           240542  OK        3211a06964d8557cb58dc6a270b050bd
bootrom_uncmp.hex     1982050 OK        dd0b9da60b1dfe093072ded8def3ebad
sysInit.out           210292  OK        300a7d3917216ec2e7496aca47f2483b
crashDump.out         14019   OK        76861fee62b29bd9b97f9f9a5d253c81
snmp_trapfuncs.out    554     OK        e8e18bcc4c3ba1146ee48a0ad92fa7af
nuEvents.out          18555   OK        3da8de0cc6d45ee0718ac5a1d32058ee
ha.out                40192   OK        443298870c441e39bad8382b62875943
confNode.out          12237   OK        74a48c89bee7909acca4deddd911fb39
authServer.out        31899   OK        1bb37d8b2e4d67832c2f55f8d62d34ca
drv.out               31016   OK        5f44307b7e53e40f29001a4283509000
qlogic.out            489356  OK        698067006ce125cc9be243bad2763abc
qlpt.out              83569   OK        23e03f4ff2f050b666c68b5bba4d6220
i82543.out            59246   OK        6c2ffcb13ef750ff5dfd0274fbc58026
smlApi.out            31018   OK        6a737f9df89c598ef0261e84421a5359
vtp.out               17215   OK        cba9a0a1168f95298525631c9e6188c2
```


scsiTargetFE.out	88822	OK	377ded7893165332e86a7c96d93b80d9
scsiTargetBE.out	49141	OK	fae10864fcf9d8cf4d3a297cc0056454
virtdev.out	303	OK	ce37770b184c0a2bdbc47fb3e5658843
scsiTcpAuth.out	8424	OK	cee026cfeb1c1624a94e26b77bf848e2
scsiTcpServer.out	102505	OK	932eeab0c617fd5ed73a010316b2f551
scsiTcpClient.out	69382	OK	fcec601fb7860c38619715b1ce037c9c
ttcp.out	22137	OK	5d596240993cbf6de71df41dbe3bd0dd
confMgmt.out	6848	OK	30f69d677a7674b5a92f156845a8a986
hdwmon.out	12941	OK	87c93f92da43619259acc5cfc5961019
diag.out	81158	OK	cf563228d268d18fb350edf42d849125
confXML.out	48350	OK	7de86cabb534da9af356e8664140c94
confObj.out	163103	OK	eb0c2c68679b34c57ccb006ef36369d9
openssl.out	515430	OK	80748cb3d9d7612e8be3f3fe4fcbe735
openssl.out	192180	OK	e99e62aaf3ce8b4e05662089eaf68eaf
clusterApp.out	23404	OK	7412b137225f425ce73f9c752ffa10c1
cdp.out	27094	OK	d06cd80dd8b3b85bb25c45cf0f597069
systemApp.out	98629	OK	27667fecc8d270e8f79747a2ad75883c
ipRouter.out	16272	OK	9cfc531fc6c22aa0200e67c88ee2f531
srMon.out	14498	OK	3c7237e46a412c2677c3e5d04e0d31e7
scsiRouter.out	64024	OK	0d6fba40d4f99bf0b530c670c8b9377f
frameRacer.out	24943	OK	86c7c0125f49dc10f2bf7c16a3ad18cd
authServerApp.out	19161	OK	d668e5ccc60e08e5337e84c510d9faa9
fcSwApp.out	57192	OK	8088e0658387e3d60148b611baac21f6
fdisk.out	14261	OK	5d005976ef3f5d78a2f0c8d75eccb0ca
sysMon.out	3218	OK	cd52039491e1c180c9755cf7b09b640b
ui.out	1422297	OK	f418df3095c77d12863d623a6000daf8
snmp_util.out	2892	OK	1bd6515766e6bc3240a115a4710ff238
mib2.out	24520	OK	c16353f4c3fc9701964b48d061f649b9
ifx.out	8995	OK	5e2816c6eae3cebafb2e8a2a794f6d8
ether.out	3712	OK	df5d6984ed1d2c5c1bb65f56771c33af
mau_if.out	5240	OK	9b1cbc21174f7f5295d178598ac661e8
mau_neg.out	3239	OK	eab35f86fb247718026b674c449a2b8a
entity.out	8358	OK	712c38391842f1fdca3b0dbf90a9ac91
entity_sensor.out	5170	OK	67d0bda3b45a6dc283477bf5e4956d93
cdp_snmp.out	6957	OK	6321d9b6ce2efb635120a7389bca6973
iscsi_mib.out	21170	OK	a91cb9c0409701b8f3aeb7909b88897f
fcmgmt_fcs.out	24181	OK	23e125253b7698f744044cce1ec60b28
fcmgmt.out	22271	OK	b52d9b4b9c0e1bf4698bab06e47f8619
snmpApp.out	3751	OK	508c923df0bfb1a7466ce9af392b482a

Disk Space (required/available): 4185180/31494144 bytes

Required switch version: (V1.4-43-0) [code=0x0104002b]

Active switch version: (V1.4.0.43-0) [code=0x0104002b]

Fallback switch version: (V1.4.3.2-0) [code=0x01040302]

Mar 18 17:38:17: %UI-5-SV: Switch Version: [V1.4.0.43-0]

Please do *NOT* shutdown or reboot the system until the software update process completes. A fatal error could occur if you shutdown or reboot the system before the software update process completes.

Attempt 1:

Gathering system files...

Verifying checksums... OK

Updating system files. OK

Updating flash device. File [/ata0/software/3.3.1-K9/bootrom_uncmp.hex] opened successfully.

Done reading.

Mar 18 17:39:47: %UI-5-SSWV5: Software activation passed: 3.3.1-K9

The software update process was successful. You must reboot the system in-order for the new software version to take effect.

Related Commands	Command	Description
	delete software version	Remove the specified version of software from the storage router.
	download software	Download the list of available software versions or the specified version of software from the named location.
	save all	Save all configuration information, including default download location for updated SN 5428-2 software.
	save system	Save selected system configuration information, including default download location for updated SN 5428-2 software.
	show software version	Display a list of software versions available on the storage router, including the currently running version and the version that will run the next time the storage router is restarted.
	software http url	Specify the default location from which to download updated SN 5428-2 software via HTTP.
	software http username	Configure the user name and optional password required to access the default download location.
	software proxy	Configure HTTP proxy information.
	software proxy url	Specify the default location from which to download updated SN 5428-2 software via HTTP, using a proxy server.
	software proxy username	Configure the user name and optional password required to access the proxy URL.
	software tftp	Specify the default location from which to download updated SN 5428-2 software via TFTP.
	verify software version	Check the specified software version for problems.

ssh enable

To enable Secure Shell (SSH) for the SN 5428-2 Storage Router and to start the SSH service, use the **ssh enable** command. To disable SSH and stop the SSH service, use the **no** form of this command.

ssh enable

no ssh enable

Syntax Description This command has no arguments or keywords.

Defaults SSH is enabled and the SSH service is started by default.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use this command to enable SSH for the storage router and start the SSH service. SSH can be used in place of Telnet to access the SN 5428-2 for management sessions.

If the SSH server is enabled and the SSH service is running, you can still restrict SSH access to the SN 5428-2 for specific interfaces by using the **restrict** command.

Examples The following example disables SSH and terminates the SSH service:

```
[SN5428-2A]# no ssh enable
*[SN5428-2A]# Jul 26 10:14:48: %UI-5-SSHAST: Stopping SSH service
```

The following example enables SSH and starts the SSH service:

```
[SN5428-2A]# ssh enable
[SN5428-2A]# Jul 26 10:14:55: %UI-5-SSSHS: Starting SSH service
```

Related Commands	Command	Description
	restrict	Secure access to storage router interfaces by communications protocols and services.
	show ssh	Display SSH server configuration.
	show ssh fingerprint	Display SSH key generation status and current public key information.
	ssh keygen	Generate the SSH public and private key pairs for the storage router.

ssh keygen

To generate the SSH public and private key pair for the SN 5428-2 Storage Router, use the **ssh keygen** command.

ssh keygen [bits *nn*]

Syntax Description	bits <i>nn</i>	Specify the number of bits to be used for the key encryption. Enter a value in the range of 512 to 3072. The default is 1024 bit.
Defaults	1024 bit public and private keys are generated for the storage router.	
Command Modes	Administrator or Monitor.	
Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

The SN 5428-2 Storage Router supports Secure Shell (SSH) protocol (version 2) as a replacement for Telnet for management sessions. SSH is a de-facto standard replacement for traditional Rlogin and Telnet that provides heavy-duty encryption and authentication for interactive sessions.

The storage router supports a single SSH management session. SSH is enabled by default, but connections are not accepted until host keys are generated using the **ssh keygen** command. SSH connections accept the Monitor mode login for authentication only; you must issue the **enable** CLI command to gain Administrator access.

If the SSH server is enabled and the SSH service is running, you can still restrict SSH access to the storage router for specific interfaces by using the **restrict** command.

After generating public/private key pairs, use the **show ssh fingerprint** command to display SSH key generation status and the current key information.

Examples

The following is example output from the **ssh keygen** command, followed by the **show ssh fingerprint** command. By default, the host key pair is generated using 1024-bit encryption.

```
[SN5428-2A]# ssh keygen
Generating all 1024 bit public/private key pairs

The time to complete this operation will vary with the key size.
Use 'show ssh fingerprint' to display status.

[SN5428-2A]# show ssh fingerprint
Key generation status is 'Idle'

1024 da:35:91:9a:fe:70:20:a7:b0:2f:d2:0e:b1:6c:6f:10 admin@SN5428-2A
1024 7f:5e:95:9c:3b:cc:10:eb:62:76:a4:88:48:08:2c:de /ata3/ssh/ssh_host_rsa_key.pub
1024 10:a6:aa:52:6a:ac:44:8a:6f:5f:21:2e:6b:1a:da:fa /ata3/ssh/ssh_host_dsa_key.pub
```


Related Commands	Command	Description
	restrict	Secure access to storage router interfaces by communications protocols and services.
	show ssh	Display SSH server configuration.
	show ssh fingerprint	Display SSH key generation status and current public key information.
	ssh enable	Enable SSH and start the SSH service.

tacacs-server host

To specify a TACACS+ server to be used for AAA authentication services, use the **tacacs-server host** command. Use the **no** form of this command to delete the specified host.

```
tacacs-server host ip-address [auth-port port-number] [timeout seconds] [key key-string]

no tacacs-server host ip-address [auth-port nn]
```

Syntax Description

<i>ip-address</i>	The IP address of the TACACS+ server.
auth-port <i>port-number</i>	(Optional) The server port number. Valid port numbers range from 1 to 65535. If unspecified, the port number defaults to 49.
timeout <i>seconds</i>	(Optional) The amount of time the storage router should wait for a reply from a TACACS+ server before timing out. This setting overrides the global setting of the tacacs-server timeout command. If no timeout value is specified, the global value is used.
key <i>key-string</i>	(Optional) The authentication and encryption key for all TACACS+ communication between the storage router and this TACACS+ server. The character string must match the key used by the TACACS+ daemon. This key overrides the global setting of the tacacs-server key command. If no key string is specified, the global value is used. If spaces are part of the key string, enclose the string in quotation marks.

Defaults

No TACACS+ server is specified.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

AAA authentication services are used to provide iSCSI authentication for IP hosts requesting access to storage resources.

- You can use multiple **tacacs-server host** commands to specify multiple TACACS+ servers. The software searches for servers in the order in which you specify them.
- If no server-specific timeout or key values are specified, the global values apply to each TACACS+ server.
- If you use spaces in the key, enclose the key in quotation marks.

Use the **aaa group server tacacs+ server** command to add a TACACS+ server to a server group. If you delete a TACACS+ server, delete the server from the TACACS+ server using the **no aaa group server tacacs+ server** command.

**Note**

Verification of IP addresses in a server group occurs only at runtime. If a TACACS+ server group contains an IP address that is not defined as a TACACS+ server, the authentication process generates error messages and the IP address is skipped. This could cause unexpected authentication failures.

Examples

The following example specifies the server with IP address 172.29.39.46 as the TACACS+ server and uses the default port for authentication:

```
[SN5428-2A] # tacacs-server host 172.29.39.46
```

The following example specifies port 52 as the destination port for authentication requests on the TACACS+ server 172.29.39.46:

```
[SN5428-2A] # tacacs-server host 172.29.39.46 auth-port 52
```

The following example specifies the server with IP address 172.29.39.46 as the TACACS server, uses ports 52 as the authorization port, sets the timeout value to 6, and sets *tac123* as the encryption key, matching the key on the TACACS+ server:

```
[SN5428-2A] # tacacs-server host 172.29.39.46 auth-port 52 timeout 6 key tac123
```

Related Commands

Command	Description
aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
aaa test authentication	Enable testing of the specified AAA authentication list.
debug aaa	Enable debugging for the AAA authentication services.
ip tacacs sourceinterface	Specify a single network interface to be used as the source IP address for all outgoing AAA authentication requests to TACACS+ servers.
radius-server host	Configure remote RADIUS servers for AAA authentication services.
restore aaa	Restore AAA authentication services from the named configuration file.
save aaa	Save the current AAA configuration information.
scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
show aaa	Display AAA configuration information.
tacacs-server key	Sets the global authentication and encryption key for all TACACS+ communications between the storage router and the TACACS+ daemon.
tacacs-server timeout	Sets the interval the storage router waits for a TACACS+ server to reply.

tacacs-server key

To set the authentication and encryption key used for all TACACS+ communications between the SN 5428-2 Storage Router and the TACACS+ daemon, use the **tacacs-server key** command. To disable the key, use the **no** form of this command.

tacacs-server key *key-string*

no tacacs-server key

Syntax Description	<i>key-string</i>	The authentication and encryption key string to be used for all TACACS+ communications, in unencrypted text. If spaces are part of the key string, enclose the string in quotation marks.
--------------------	-------------------	---

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>3.2.1.</td><td>This command was introduced.</td></tr></table>	Release	Modification	3.2.1.	This command was introduced.
Release	Modification				
3.2.1.	This command was introduced.				

Usage Guidelines	<p>After using the aaa authentication iscsi command to configure the iSCSI authentication list to use TACACS+ authentication services, use the tacacs-server key command to set the global authentication and encryption key. The key entered as part of the command must match the key used on the TACACS+ daemon. If spaces are part of the key string, enclose the key string in quotation marks.</p> <p>To override the global key for a specific TACACS+ server, use the tacacs-server host command with the key keyword.</p>
------------------	--

Examples	<p>The following example sets the global authentication and encryption key to <i>my TACACS key string</i>:</p> <pre>[SN5428-2A] # radius-server key "my TACACS key string"</pre>
----------	--

Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
	aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	debug aaa	Enable debugging for the AAA authentication services.
	ip tacacs sourceinterface	Specify a single network interface to be used as the source IP address for all outgoing AAA authentication requests to TACACS+ servers.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.
	tacacs-server timeout	Sets the interval the storage router waits for a TACACS+ server to reply.

tacacs-server timeout

To set the global interval that the SN 5428-2 Storage Router waits for a TACACS+ server to reply, use the **tacacs-server timeout** command.To restore the default, use the **no** form of this command.

tacacs-server timeout *seconds*

no tacacs-server timeout

Syntax Description	<i>seconds</i>	The global timeout value, in seconds. Enter a value in the range of 1 to 1000. The default is 5.
--------------------	----------------	--

Defaults	The timeout value defaults to five seconds.
----------	---

Command Modes	Administrator.
---------------	----------------

Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>3.2.1</td><td>This command was introduced.</td></tr></table>	Release	Modification	3.2.1	This command was introduced.
Release	Modification				
3.2.1	This command was introduced.				

Usage Guidelines	<p>Use this command to set the number of seconds the storage router waits for a TACACS+ server to reply before timing out.</p> <p>To override the global timeout value for a specific TACACS+ server, use the tacacs-server host command with the timeout keyword.</p>
------------------	--

Examples	<p>The following example sets the global timeout value to 10. You may want to increase the timeout value if you have network problems or if TACACS+ servers are slow to respond, causing persistent timeouts when a lower timeout value is used.</p> <pre>[SN5428-2A] # tacacs-server timeout 10</pre>
----------	--

Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
	aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	debug aaa	Enable debugging for the AAA authentication services.
	ip tacacs sourceinterface	Specify a single network interface to be used as the source IP address for all outgoing AAA authentication requests to TACACS+ servers.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.
	tacacs-server key	Sets the global authentication and encryption key for all TACACS+ communications between the storage router and the TACACS+ daemon.

telnet enable

To enable Telnet for the SN 5428-2 Storage Router and to start the Telnet server, use the **telnet enable** command. To disable Telnet and stop the Telnet server, use the **no** form of this command.

telnet enable

no telnet enable

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Defaults	Telnet is enabled and the Telnet server is started by default.
-----------------	--

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	<p>Use this command to enable Telnet for the storage router and start the Telnet server.</p> <p>If Telnet is enabled and the Telnet server is running, you can still restrict Telnet access to the storage router for specific interfaces by using the restrict command.</p>
-------------------------	---

Examples	<p>The following example disables Telnet and stops the Telnet server:</p> <pre>[SN5428-2A] # no telnet enable</pre> <p>The following example enables Telnet and starts the Telnet server:</p> <pre>[SN5428-2A] # telnet enable</pre>
-----------------	--

Related Commands	Command	Description
	restrict	Secure access to storage router interfaces by communications protocols and services.
	show telnet	Display the status of the Telnet server.

username password

To build a local user name database for use with the local method of AAA authentication services, use the **username password** command. Use the **no** form of this command to delete the specified user name.

username *user-name* **password** *password-string*

no username *user-name*

Syntax Description

<i>user-name</i>	A valid user name. Enter a maximum of 63 characters.
<i>password-string</i>	The password associated with the specified user name. If the password is encrypted (starts with “9”), enter a maximum of 170 characters. If the password is unencrypted (starts with “0”), enter a maximum of 66 characters. If the password is entered as an unencrypted text string, enter a maximum of 64 characters.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use the **username password** command to build the local username database. The AAA authentication service, *local-case*, performs a case-sensitive user name match; the *local* service user name match is not case-sensitive. Both *local* and *local-case* use case-sensitive password matching for authentication.

Use the **aaa authentication iscsi** or **aaa authentication login** command to configure the authentication list to use *local* or *local-case* authentication services.

To display the contents of the local username database, issue the **show aaa** command.

The following rules apply to passwords:

- Passwords are entered in clear text. However, they are changed to “XXXXXX” in the CLI command history cache, and are stored in the local username database in an encrypted format.
- If the password contains embedded spaces, enclose it with single or double quotes.
- After initial entry, passwords display in their encrypted format. Use the **show aaa** command to display the local username database entries. The following is an example display:

```
username "foo" password "9 ea9bb0c57ca4806d3555f3f78a4204177a"
```

The initial “9” in the example display indicates that the password is encrypted.

- You can re-enter an encrypted password using the normal **username password** command. Enter the encrypted password in single or double quotes, starting with 9 and a single space. For example, copying and pasting `password "9 ea9bb0c57ca4806d3555f3f78a4204177a"` from the example above into the **username pat** command would create an entry for *pat* in the username database. The user named *pat* would have the same password as the user named *foo*. This functionality allows user names and passwords to be restored from saved configuration files.
- When entering a password, a zero followed by a single space indicates that the following string is not encrypted; 9 followed by a single space indicates that the following string is encrypted. To enter a password that starts with 9 or zero, followed by one or more spaces, enter a zero and a space and then enter the password string. For example, to enter the password “0 123” for the user named *pat*, enter this command:

```
username pat password "0 0 123"
```

To enter the password “9 73Zjm 5” for user name *lab1*, use this command:

```
username lab1 password '0 9 73Zjm 5'
```

Examples

The following example configures two user names (*foo* and *foo2*) and password (*foopassword* and *foo2password*):

```
[SN5428-2A]# username foo password foopassword
[SN5428-2A]# username foo2 password foo2password
```

To display the user name database, issue the **show aaa** command. The following is example output from the **show aaa** command:

```
[SN5428-2A]# show aaa
aaa new-model
aaa authentication iscsi default group tacacs+ local none
username foo password <password>
username foo2 password <password>
```

Related Commands

Command	Description
aaa authentication enable	Configure AAA authentication services for Administrator mode access to the SN 5428-2 Storage Router via the CLI enable command.
aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
aaa authentication login	Configure AAA authentication services for Monitor mode access to the SN 5428-2 Storage Router via the CLI.
aaa generate password	Generate a long random password.
aaa test authentication	Enable testing of the specified AAA authentication list.
debug aaa	Enable debugging for the AAA authentication services.
restore aaa	Restore AAA authentication services from the named configuration file.
save aaa	Save the current AAA configuration information.
scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
show aaa	Display AAA configuration information.

verify software version

To check the specified software version for problems, issue the **verify software version** command.

verify software version {*version-id* | **all** | **boot** | **current**}

Syntax Description		
<i>version-id</i>		A specific version of software, which must be available to the storage router.
all		Verify all software versions available to the storage router.
boot		The software version that is set to boot at the next system restart.
current		The software version that is currently running.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Use this command after downloading software to verify that the download completed successfully and that the downloaded software is bootable. The size and the status of each module is verified.

Examples The following is example output from the **verify software version** command:

```
[SN5428-2A]# verify software version 3.3.1-K9
```

Module	Size	Status	MD5 Digest
vxWorks	3538310	OK	8eedbb49e12069825d90966d5ea97a74
vxWorks.sym	240542	OK	afbd05b7723a70c3c2eeafde1c13ec90
bootrom_uncmp.hex	1982185	OK	ecc6f45364e76702419cee1246737a3a
sysInit.out	210292	OK	a250add5f1358c94631ff5f91103e247
crashDump.out	14019	OK	76861fee62b29bd9b97f9f9a5d253c81
snmp_trapfuncs.out	554	OK	e8e18bcc4c3ba1146ee48a0ad92fa7af
nuEvents.out	18554	OK	d90d609ef8ad44b60d80ae9ac2ac0ea7
ha.out	40192	OK	443298870c441e39bad8382b62875943
confNode.out	12237	OK	74a48c89bee7909acca4deddd911fb39
authServer.out	31899	OK	1bb37d8b2e4d67832c2f55f8d62d34ca
drv.out	31016	OK	5f44307b7e53e40f29001a4283509000
qllogic.out	489130	OK	d9050e9fccfcc0f0e2c0ec2386b63acc
qlpt.out	83569	OK	23e03f4ff2f050b666c68b5bba4d6220
i82543.out	59246	OK	6c2ffcb13ef750ff5dfd0274f5e58026
smlApi.out	31018	OK	6a737f9df89c598ef0261e84421a5359
vtp.out	17215	OK	cba9a0a1168f95298525631c9e6188c2
scsiTargetFE.out	88754	OK	6c3daf47e5e2dbd2911fd86df28826e3
scsiTargetBE.out	49141	OK	fae10864fcf9d8cf4d3a297cc0056454

verify software version

virtdev.out	303	OK	ce37770b184c0a2bdbc47fb3e5658843
scsiTcpAuth.out	8424	OK	cee026cfeb1c1624a94e26b77bf848e2
scsiTcpServer.out	102480	OK	263b94e089979b927afd8cecb14f988f
scsiTcpClient.out	69382	OK	fcec601fb7860c38619715b1ce037c9c
ttcp.out	22137	OK	5d596240993cbf6de71df41dbe3bd0dd
confMgmt.out	6848	OK	30f69d677a7674b5a92f156845a8a986
hdwmon.out	12941	OK	87c93f92da43619259acc5cfc5961019
diag.out	78975	OK	0368ebbee6bdf89cb7ed98e597be9ae
confXML.out	48350	OK	7de86cabbe534da9af356e8664140c94
confObj.out	163180v	OK	985bc57d5c5dd32cead34cd401c84e07
openssl.out	515026	OK	1109b92a3efcbf26689f25a1bf7993a0
openssh.out	191979	OK	f7d00201642055e6277d2a770b44e8eb
clusterApp.out	23404	OK	7412b137225f425ce73f9c752ffa10c1
cdp.out	27094	OK	d06cd80dd8b3b85bb25c45cf0f597069
systemApp.out	98629	OK	27667fecc8d270e8f79747a2ad75883c
ipRouter.out	16272	OK	9cfc531fc6c22aa0200e67c88ee2f531
srMon.out	14498	OK	3c7237e46a412c2677c3e5d04e0d31e7
scsiRouter.out	64023	OK	162d920a21dd8fe54884ef652c0eb30a
frameRacer.out	24943	OK	86c7c0125f49dc10f2bf7c16a3ad18cd
authServerApp.out	19161	OK	d668e5ccc60e08e5337e84c510d9faa9
fcSwApp.out	54609	OK	0314888330be2e0fb59083f54e27db48
fdisk.out	14261	OK	5d005976ef3f5d78a2f0c8d75eccb0ca
sysMon.out	3218	OK	cd52039491e1c180c9755cf7b09b640b
ui.out	1418774	OK	ccb23ff8c71d803a02f358e409d28948
snmp_util.out	2892	OK	1bd6515766e6bc3240a115a4710ff238
mib2.out	24520	OK	c16353f4c3fc9701964b48d061f649b9
ifx.out	8995	OK	5e2816c6eaec3cebafeb2e8a2a794f6d8
ether.out	3712	OK	df5d6984ed1d2c5c1bb65f56771c33af
mau_if.out	5240	OK	9b1cbc21174f7f5295d178598ac661e8
mau_neg.out	3239	OK	eab35f86fb247718026b674c449a2b8a
entity.out	8358	OK	712c38391842f1fdca3b0dbf90a9ac91
entity_sensor.out	5170	OK	67d0bda3b45a6dc283477bf5e4956d93
cdp_snmp.out	6957	OK	6321d9b6ce2efb635120a7389bca6973
iscsi_mib.out	21171	OK	7b1977f687ffb3f23272eb04f1d03bb7
fcmgmt_fcsw.out	24181	OK	23e125253b7698f744044cce1ec60b28
fcmgmt.out	22271	OK	15de1b02953f6e10c01362553ed28e75
snmpApp.out	3751	OK	508c923df0bfb1a7466ce9af392b482a

Related Commands

Command	Description
delete software version	Remove the specified version of software from the storage router.
download software	Download the list of available software versions or the specified version of software from the named location.
show software version	Display a list of software versions available on the storage router, including the currently running version and the version that will run the next time the storage router is restarted.

vlan

To configure a VLAN on the SN 5428-2 Storage Router, use the **vlan** command. To delete a VLAN, use the **no vlan** form of this command.

vlan *vid* [**name** *vlan_name*] [**mtusize** *nn*]

no vlan *vid* [**force**]

Syntax Description	<i>vid</i>	VLAN identification (VID) number. Enter an integer from 1 to 4095.
	name <i>vlan_name</i>	(Optional) The name of the VLAN, which can be up to 32 characters in length. If not specified, the default VLAN name has <i>VLAN</i> as the prefix followed by the VID, left padded to four bytes (for example, VLAN0002, or VLAN0045).
	mtusize <i>nn</i>	The size of the maximum transfer unit, in bytes. <i>nn</i> is an integer from 1500 to 9000. The default MTU is 1500.
	force	(Optional) Keyword that overrides normal protections, allowing the action to be performed.

Defaults The default VLAN name is comprised of the prefix *VLAN* and the VID, left padded to four bytes. The default MTU size is 1500.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.
	3.3.1	The force keyword was added.

Usage Guidelines In a cluster environment, VLAN management functions are handled by a single storage router. To determine which storage router is performing VLAN management functions, issue the **show cluster** command. If you issue the **vlan** command from a storage router that is not performing VLAN management functions, the CLI displays an informational message with the name of the node that is currently handling those functions. See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about operating the storage router in a cluster.

VLANs are a cluster-wide configuration item. When configured and saved to the bootable configuration, HA communications will propagate the VLAN information to all storage routers in the cluster. You can configure a maximum of 16 logical interfaces (VLANs associated with IP addresses) per physical Gigabit Ethernet interface in the SN 5428-2 or cluster.

VLAN information can only be configured when the storage router is in VTP Transparent mode. In transparent mode, received VTP packets are ignored and VLAN configuration information is retrieved from the high availability cluster.

The storage router uses 802.1Q VLAN encapsulation to carry VLAN information on packets sent and received on the Gigabit Ethernet interface. The 802.1Q packet tag is a four-byte field inserted between the source MAC address and ether-type fields in the layer 2 header. It consists of a two-byte Tag Protocol Identifier (TPID) field and a two-byte Tag Control Information (TCI) field. The TPID contains the “protocol type” field (0x8100), which identifies the packet as a valid 802.1Q tagged packet. The TCI contains the 12-bit VLAN Identifier (VID) field and a 3-bit User Priority (UP) field.

Use the **vlan** command to locally configure VLANs when the storage router is connected to a switched network that does not support VTP but does support 802.1Q VLANs.

VLANs can only be deleted if they are not in use. Use the **force** keyword to bypass this restriction and delete a VLAN that is currently in use.

Examples

The following set of commands places the storage router in VTP Transparent mode and configures a VLAN named *weblan001* on the storage router. The VID is 45.

```
[SN5428-2A]# vtp mode transparent
[SN5428-2A]# Jul 30 15:24:02:Vtp:AS_NOTICE :VTP changed to transparent mode
[SN5428-2A]# vlan 45 name weblan001
[SN5428-2A]# Jul 30 15:25:45:Vtp:AS_NOTICE :VLAN 45 added (name=VLAN0045, mtu=1500)
```

Related Commands

Command	Description
restore vlan	Restore VLAN configuration information from the named configuration file.
save all	Save all configuration information, including VLAN information.
save scsirouter	Save configuration information for the named SCSI routing instance.
save system	Save selected system configuration information, including VLAN information.
save vlan	Save configuration information for the named VLAN or all VLANs.
scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
show vlan	Display configuration and operational information for the specified VLAN or all VLANs.
show vtp	Display configuration and operational information for VTP.
vtp domain	Assign a VTP domain name to the storage router.
vtp mode	Configure the storage router to operate in client or transparent VTP mode.

vtp domain

To assign a VLAN Trunking Protocol (VTP) domain name to the SN 5428-2 Storage Router, use the **vtp domain** command. VLAN information will not be accepted from a switch which is in a different domain.

vtp domain {*domain_name* | **none**}

Syntax Description	<i>domain_name</i>	The name of the domain to which the storage router belongs.
	none	The storage router is not assigned to a specific domain. If the storage router is in VTP Client mode, it will assign itself to the first domain from which it receives a VTP message. This is the default.

Defaults	None. The storage router will assign itself to the first domain from which it receives a VTP message.
----------	---

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	<p>In a cluster environment, VTP configuration functions are handled by a single storage router. To determine which storage router is performing VTP configuration functions, issue the show cluster command. The storage router that is performing VLAN management also performs VTP configuration. If you issue the vtp domain command from a storage router that is not performing VTP configuration functions, the CLI displays an informational message with the name of the node that is currently handling those functions. See Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,” for more information about operating the storage router in a cluster.</p>
------------------	---

The VTP domain name applies to all storage routers participating in a cluster. The VTP domain name is a cluster-wide configuration setting. When the VTP domain name is set using the **vtp domain** command and saved to the boot configuration file (via a **save all** or **save system** command), an HA exchange occurs and the VTP domain name will become active on all storage routers in the cluster.

Examples	The following example sets the VTP domain name to <i>Lab_Network</i> :
----------	--

```
[SN5428-2A]# vtp domain Lab_Network
```


Related Commands	Command	Description
	restore vlan	Restore VLAN configuration information from the named configuration file.
	save all	Save all configuration information, including VLAN information.
	save scsirouter	Save configuration information for the named SCSI routing instance.
	save system	Save selected system configuration information, including VLAN information.
	save vlan	Save configuration information for the named VLAN or all VLANs.
	scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
	show vlan	Display configuration and operational information for the specified VLAN or all VLANs.
	show vtp	Display configuration and operational information for VTP.
	vlan	Configure a non-VTP VLAN on the storage router.
	vtp mode	Configure the storage router to operate in client or transparent VTP mode.

vtp mode

To assign the VTP mode in which the SN 5428-2 Storage Router operates, use the **vtp mode** command.

vtp mode {client | transparent}

Syntax Description	client	The storage router will operate in VTP Client mode. It will exchange VTP packets with an externally attached switch to learn about the VLANs that are accessible in the network. This is the default.
	transparent	The storage router will operate in VTP Transparent mode. It will not exchange VTP packets and will only learn about VLANs from explicit storage router configuration via the vlan command.

Defaults	Client.
----------	---------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines

In a cluster environment, VTP configuration functions are handled by a single storage router. To determine which storage router is performing VTP configuration functions, issue the **show cluster** command. The storage router that is performing VLAN management also performs VTP configuration. If you issue the **vtp mode** command from a storage router that is not performing VTP configuration functions, the CLI displays an informational message with the name of the node that is currently handling those functions. See [Chapter 11, “Maintaining and Managing the SN 5428-2 Storage Router,”](#) for more information about operating the storage router in a cluster.

VTP operates in either client or transparent mode. In client mode, the storage router exchanges VTP packets with a locally connected switch to learn about the VLANs available in the network. In transparent mode, VTP packets are ignored and VLAN information is pulled directly from the storage router cluster configuration.

When operating as a VTP client, the storage router sends a VTP advertisement when one of the following events occur:

- The Gigabit Ethernet interface on any storage router in the cluster transitions to the *up* state and a valid domain name has either been configured or previously learned.
- The VTP domain name changes.
- A VTP summary advertisement is received with a higher configuration revision.

The switch replies to the storage router with a summary advertisement, followed by one or more subset advertisements.

When operating in transparent mode, the storage router ignores any VTP packets it may receive. VLANs are configured using the GUI or the CLI **vlan** command. Use transparent mode when the storage router is connected to a switched network that does not support VTP but does support 802.1Q VLANs.

Examples

The following example places the storage router in VTP Transparent mode:

```
[SN5428-2A] # vtp mode transparent
```

Related Commands

Command	Description
restore vlan	Restore VLAN configuration information from the named configuration file.
save all	Save all configuration information, including VLAN information.
save scsirouter	Save configuration information for the named SCSI routing instance.
save system	Save selected system configuration information, including VLAN information.
save vlan	Save configuration information for the named VLAN or all VLANs.
scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
show vlan	Display configuration and operational information for the specified VLAN or all VLANs.
show vtp	Display configuration and operational information for VTP.
vlan	Configure a non-VTP VLAN on the storage router.
vtp domain	Assign a VTP domain name to the storage router.

zone

To create a Fibre Channel (FC) switched fabric zone, use the **zone** command.

zone *name*

Syntax Description	<i>name</i>	The name of the zone created by this command. Enter a maximum of 31 characters. The name must begin with an alpha character.
--------------------	-------------	--

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	FC fabric zoning enables you to divide ports and devices of the FC fabric into zones to provide more efficient and secure communication among grouped nodes. Zones are named groups of ports or devices that can communicate with each other. Zone membership can be defined by World Wide Port Name (WWPN), port number or FC address. The storage router supports zone membership defined by WWPN (or alias) only.
------------------	--

Zone members can only communicate with other members in the same zone; however, a port or device can be a member of multiple zones.



Caution

If the storage router is connected to the FC switched fabric, all zoning changes (including the creation of a new FC zone) are immediately propagated to other SN 5428-2 Storage Routers and switches in the fabric.

See [Chapter 5, “Configuring Fibre Channel Interfaces,”](#) for more information about FC switched fabric zones.

Examples	The following example creates a zone named <i>labzone3</i> :
----------	--

```
[SN5428-2A] # zone labzone3
```


Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	delete zone	Delete the specified Fibre Channel zone or the specified member of the zone from the zoning database.
	delete zoneset	Delete the specified zone from the zone set or to delete the entire named zone set from the zoning database.
	fcalias	Create an alias entity for use in Fibre Channel zoning.
	fcalias member	Add the specified member to the named alias.
	fcswitch zoning autosave	Enable the SN 5428-2 Storage Router to save zoning changes received from switches in the fabric.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	fcswitch zoning merge	Set zoning merge compliance.
	show debug fcswitch	Display internal Fibre Channel interface parameters.
	show fcalias	Display information about aliases and their members.
	show fcswitch	Display global configuration information for storage router FC interfaces.
	show fcswitch fabric	Display information about the Fibre Channel fabric.
	show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
	show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
	zone member	Add a device or an alias to a zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset enable	Activate a zone set.
	zoneset zone	Add a member zone to a zone set.

zone member

To add a device or an alias to a zone, use the **zone member** command.

zone name member {fcalias alias-name | wwpn xxxxxxxxxxxxxxxx}

Syntax Description	
<i>name</i>	The name of the zone to which the member is being added.
fcalias <i>alias-name</i>	Make the specified alias a member of the named zone.
wwpn xxxxxxxxxxxxxxxx	Make the specified WWPN a member of the named zone.
Note	WWPN address notation is represented by 16 hex digits. The digits may be separated by colons. When entering WWPN addresses, colons can be omitted or placed anywhere in the address notation as long as they do not leave one character without a partner character.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines Zones are named groups of ports or devices that can communicate with each other. A zone member can be a port or a device associated with a specific WWPN, or an alias. An alias is a named set of ports or devices that are grouped together for convenience. You can add a WWPN or an alias to one or more zones.

Zone members can only communicate with other members in the same zone; however, a port or device can be a member of multiple zones.



Caution

If the storage router is connected to the Fibre Channel (FC) switched fabric, all zoning changes (including adding a member to a zone) are immediately propagated to other SN 5428-2 Storage Routers and switches in the fabric.

See [Chapter 5, “Configuring Fibre Channel Interfaces,”](#) for more information about fabric zones.

Examples

The following example adds the aliases *testgroup1* and *testgroup2* and the WWPN *220145ab32ca7890* to the zone named *labgroup3*:

```
[SN5428-2A] # zone labzone3 member fcalias testgroup1
[SN5428-2A] # zone labzone3 member fcalias testgroup2
[SN5428-2A] # zone labzone3 member wwpn 2201:45ab:32ca:7890
```


Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	delete zone	Delete the specified Fibre Channel zone or the specified member of the zone from the zoning database.
	delete zoneset	Delete the specified zone from the zone set or to delete the entire named zone set from the zoning database.
	fcalias	Create an alias entity for use in Fibre Channel zoning.
	fcalias member	Add the specified member to the named alias.
	fcswitch zoning autosave	Enable the SN 5428-2 Storage Router to save zoning changes received from switches in the fabric.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	fcswitch zoning merge	Set zoning merge compliance.
	show debug fcswitch	Display internal Fibre Channel interface parameters.
	show fcalias	Display information about aliases and their members.
	show fcswitch	Display global configuration information for storage router FC interfaces.
	show fcswitch fabric	Display information about the Fibre Channel fabric.
	show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
	show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
	zone	Create a Fibre Channel fabric zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset enable	Activate a zone set.
	zoneset zone	Add a member zone to a zone set.

zoneset

To create a Fibre Channel (FC) switched fabric zone set, use the **zoneset** command.

zoneset *name*

Syntax Description	<i>name</i>	The name of the zone set created by this command. Enter a maximum of 31 characters. The name must begin with an alpha character.
---------------------------	-------------	--

Defaults	None.
-----------------	-------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	A zone set is a named group of fabric zones. A zone can belong to multiple zone sets. The SN 5428-2 Storage Router and each switch in the fabric maintains its own zoning database containing one or more zone sets. When you activate a zone set, zone sets of the same name from all SN 5428-2s and switches in the fabric are compiled and then the merged active zone set is redistributed to every SN 5428-2 and switch in the fabric. This means that all switches and SN 5428-2s in the fabric have identical active zone sets.
-------------------------	--

**Caution**

If the storage router is connected to the FC switched fabric, all zoning changes (including the creation of a new FC switched fabric zone set) are immediately propagated to other SN 5428-2 Storage Routers and switches in the fabric.

See [Chapter 5, “Configuring Fibre Channel Interfaces,”](#) for more information about FC fabric zoning.

Examples	The following example creates a zone set named <i>foo</i> :
-----------------	---

```
[SN5428-2A] # zoneset foo
```


Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	delete zone	Delete the specified Fibre Channel zone or the specified member of the zone from the zoning database.
	delete zoneset	Delete the specified zone from the zone set or to delete the entire named zone set from the zoning database.
	fcalias	Create an alias entity for use in Fibre Channel zoning.
	fcalias member	Add the specified member to the named alias.
	fcswitch zoning autosave	Enable the SN 5428-2 Storage Router to save zoning changes received from switches in the fabric.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	fcswitch zoning merge	Set zoning merge compliance.
	show debug fcswitch	Display internal Fibre Channel interface parameters.
	show fcalias	Display information about aliases and their members.
	show fcswitch	Display global configuration information for storage router FC interfaces.
	show fcswitch fabric	Display information about the Fibre Channel fabric.
	show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
	show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
	zone	Create a Fibre Channel fabric zone.
	zone member	Add a device or an alias to a zone.
	zoneset enable	Activate a zone set.
	zoneset zone	Add a member zone to a zone set.

zoneset enable

To activate a zone set, use the **zoneset enable** command. To deactivate a zone set, use the **no** form of this command.

zoneset *name* **enable**

no zoneset *name* **enable**

Syntax Description	<i>name</i>	The name of the zone set being activated.
---------------------------	-------------	---

Defaults	None.
-----------------	-------

Command Modes	Administrator.
----------------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	<p>The SN 5428-2 Storage Router and each switch in the fabric maintains its own zoning database containing one or more zone sets. You must activate a zone set to apply its zoning definitions to the Fibre Channel (FC) fabric. When you activate a zone set, zone sets of the same name from all SN 5428-2s and switches in the fabric are compiled and then the merged active zone set is redistributed to every SN 5428-2 and switch in the fabric. This means that all switches and SN 5428-2s in the fabric have identical active zone sets.</p>
-------------------------	--

Only one zone set can be active at a time. You must explicitly deactivate an active zone set to allow another zone set to be activated.

**Caution**

If the storage router is connected to the FC switched fabric, all zoning changes (including activating a zone set) are immediately propagated to other SN 5428-2 Storage Routers and switches in the fabric.

See [Chapter 5, “Configuring Fibre Channel Interfaces,”](#) for more information about FC fabric zoning.

Examples	The following example activates the zone set named foo:
-----------------	---

```
[SN5428-2A] # zoneset foo enable
```


Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	delete zone	Delete the specified Fibre Channel zone or the specified member of the zone from the zoning database.
	delete zoneset	Delete the specified zone from the zone set or to delete the entire named zone set from the zoning database.
	fcalias	Create an alias entity for use in Fibre Channel zoning.
	fcalias member	Add the specified member to the named alias.
	fcswitch zoning autosave	Enable the SN 5428-2 Storage Router to save zoning changes received from switches in the fabric.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	fcswitch zoning merge	Set zoning merge compliance.
	show debug fcswitch	Display internal Fibre Channel interface parameters.
	show fcalias	Display information about aliases and their members.
	show fcswitch	Display global configuration information for storage router FC interfaces.
	show fcswitch fabric	Display information about the Fibre Channel fabric.
	show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
	show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
	zone	Create a Fibre Channel fabric zone.
	zone member	Add a device or an alias to a zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset zone	Add a member zone to a zone set.

zoneset zone

To add a member zone to a zone set, use the **zoneset zone** command.

zoneset *name* **zone** *name*

Syntax Description	<i>name</i>	The name of the zone set to which the member is being added.
	zone <i>name</i>	The name of the zone.

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	3.2.1	This command was introduced.

Usage Guidelines	<p>A zone set is a named group of fabric zones. Zones are named groups of ports or devices that can communicate with each other. Zone members are identified in the storage router by WWPN. A zone can belong to multiple zone sets.</p> <p>See Chapter 5, “Configuring Fibre Channel Interfaces,” for more information about Fibre Channel fabric zoning.</p>
------------------	--

Examples	<p>The following example adds the zone named <i>labzone3</i> to the zone set named <i>foo</i>:</p> <pre>[SN5428-2A]# zoneset foo zone labzone3</pre>
----------	--

Related Commands	Command	Description
	clear fcswitch	Clear the switch log files of all entries or clear stored zoning configuration information.
	delete zone	Delete the specified Fibre Channel zone or the specified member of the zone from the zoning database.
	delete zoneset	Delete the specified zone from the zone set or to delete the entire named zone set from the zoning database.
	fcalias	Create an alias entity for use in Fibre Channel zoning.
	fcalias member	Add the specified member to the named alias.
	fcswitch zoning autosave	Enable the SN 5428-2 Storage Router to save zoning changes received from switches in the fabric.
	fcswitch zoning default	Select the level of communication between the storage router and devices in the fabric where there is no active zone set.
	fcswitch zoning merge	Set zoning merge compliance.
	show debug fcswitch	Display internal Fibre Channel interface parameters.
	show devices	Display a variety of debug information or perform specific troubleshooting activities for Fibre Channel zones.
	show fcalias	Display information about aliases and their members.
	show fcswitch	Display global configuration information for storage router FC interfaces.
	show fcswitch fabric	Display information about the Fibre Channel fabric.
	show zone	Display configuration and operational information for Fibre Channel fabric zones from the local zoning database.
	show zoneset	Display configuration and operational information for Fibre Channel fabric zone sets.
	zone	Create a Fibre Channel fabric zone.
	zone member	Add a device or an alias to a zone.
	zoneset	Create a Fibre Channel fabric zone set.
	zoneset enable	Activate a zone set.